

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2002 年 4 月 11 日 (11.04.2002)

PCT

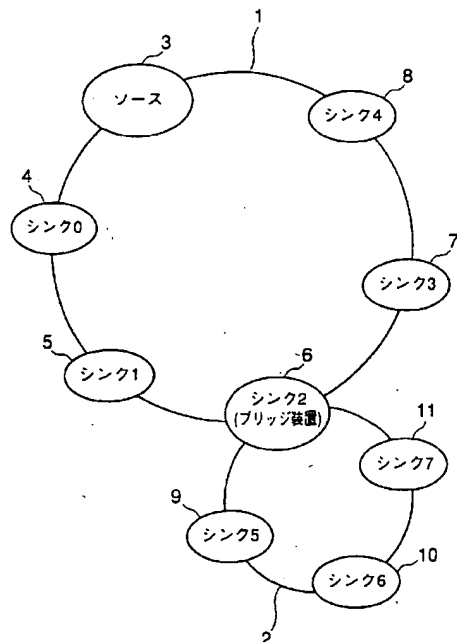
(10) 国際公開番号
WO 02/30054 A1

- (51) 国際特許分類⁷: H04L 12/28, G06F 13/00 (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006番地 Osaka (JP).
- (21) 国際出願番号: PCT/JP01/08034
- (22) 国際出願日: 2001 年 9 月 17 日 (17.09.2001)
- (25) 国際出願の言語: 日本語 (72) 発明者; および (75) 発明者/出願人 (米国についてのみ): 山田正純 (YAMADA, Masazumi) [JP/JP]; 〒543-0071 大阪府大阪市天王寺区生玉町11-14-301 Osaka (JP). 飯塚裕之 (IIT-SUKA, Hiroyuki) [JP/JP]; 〒576-0033 大阪府交野市私市6-25-6 Osaka (JP). 臼木直司 (USUKI, Naoshi) [JP/JP]; 〒614-8331 京都府八幡市橋本意足26-12 Kyoto (JP).
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2000-298590 2000 年 9 月 29 日 (29.09.2000) JP

[続葉有]

(54) Title: COPYRIGHT PROTECTIVE SYSTEM, TRANSMITTER, RECEIVER, BRIDGE DEVICE, COPYRIGHT PROTECTIVE METHOD, MEDIUM, AND PROGRAM

(54) 発明の名称: 著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラム



(57) Abstract: If a bridge device is connected to a network such as of a IEEE1394 bus, the desire of the copyright owners to limit the number of devices that can receive a signal cannot be met. A copyright protective system is characterized in that it is connected to a network and comprises one or more receivers for receiving and using data the copyright of which should be protected and a transmitter or transmitting the data the copyright of which should be protected to the receivers through the network, the transmitter (20) includes transmission-side authentication means (23) for authentication together with the receivers and authentication count means (24) for counting the authentications that the transmission-side authentication means (23) has made, and each of the receivers includes reception-side authentication means for authentication together with the transmission-side authentication means so as to limit the authentications.

- 3...SOURCE
4...SINK 0
5...SINK 1
6...SINK 2 (BRIDGE DEVICE)
7...SINK 3
8...SINK 4
9...SINK 5
10...SINK 6
11...SINK 7

[続葉有]



(74) 代理人: 弁理士 松田正道(MATSUDA, Masamichi); 添付公開書類:
〒532-0003 大阪府大阪市淀川区宮原5丁目1番3号 新 — 国際調査報告書
大阪生島ビル Osaka (JP).

(81) 指定国 (国内): JP, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, 2文字コード及び他の略語については、定期発行される
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR). 各PCTガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

(57) 要約:

IEEE 1394バスなどのネットワークにブリッジ装置が接続されると、信号を受け取られる機器の数を制限したいという著作権者の要望を守ることが出来ない。

ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも1台以上の受信装置と、受信装置に、ネットワークを利用して著作権保護が必要なデータを送信する送信装置20とを備え、送信装置20は、受信装置と認証を行う送信側認証手段23と、送信側認証手段23が認証した数である認証数を数える認証数カウント手段24とを有し、受信装置は、送信側認証手段と認証を行う受信側認証手段を有し、前記認証数に制限を設けたことを特徴とする。

明 細 書

著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラム

技術分野

本発明は、著作権保護が必要なデータの著作権を保護してデータを送受信する著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラムに関するものである。

背景技術

近年、ＡＶ機器間を接続するネットワークの技術が普及している。このようなネットワークの１つとしてＩＥＥＥ１３９４－１９９５規格（以下ＩＥＥＥ１３９４と呼ぶ）のシリアルバス（以下ＩＥＥＥ１３９４バスと呼ぶ）が存在する。ＩＥＥＥ１３９４は、シリアル伝送を行う高速バスシステムの規格であり、データを同期伝送できるため、ＡＶデータなどのリアルタイム伝送が可能である。このようなＩＥＥＥ１３９４は、家庭用デジタルＡＶ機器を始め、多くのデジタル映像音声機器に外部用インターフェースとして搭載されようとしている。

一方、新作の映画や有料放送のテレビ番組、音楽などの著作権保護が必要なデータを扱う場合、著作権を保護する必要がある。著作権を保護するための有力な方法として、著作権保護を必要とするデータを暗号化してデータの利用に制限を加える方法がある。

例えば、映像音声データ（以下ＡＶデータと記す）をＩＥＥＥ１３９４バスを利用して伝送する際、ＡＶデータを著作権保護する必要がある場合、そ

のAVデータを暗号化して伝送することが行われている。そのような例としてDTCP (Digital Transmission Content Protection) 方式が規格化されている。

DTCP方式は、認証機能と鍵の無効化機能を備えており、IEEE1394バスでデータ伝送する際に、不正な機器を排除し、AVデータなどの著作権保護が必要なデータを暗号化して伝送することにより著作権の保護を実現している。

コンテンツデータを送信する送信機は、コンテンツデータをコンテンツ鍵で暗号化する。このコンテンツ鍵は送信機により定期的に更新される。更新されるコンテンツ鍵を受信機に安全に渡すため、送信機はコンテンツ鍵を交換鍵と呼ばれる鍵で暗号化して受信機に送信する。

認証機能は暗号化されたデータを解くための鍵をDTCPのライセンスを受けた受信機にだけ渡すために行われるもので、データに付加されたコピー制限情報（「一回コピー可」「コピー不可」など）と機器の特性（記録機能あり、表示機能のみ、データ内のフォーマット解析・デコードが可能か否かなど）に応じて、公開鍵暗号技術を使用したフル認証と、共通鍵暗号を使用した制限認証を使い分ける。フル認証対応の機器はライセンス機構が付与した署名を含む証明書データを持つ。認証時には、証明書データを送受し、公開鍵暗号技術を使用した電子署名のアルゴリズムを使用して署名が正しいことを判定する。証明書データと併せて乱数を送り合うことにより、認証を行う二台の間でのみ有効な認証鍵を、両方の乱数を用いてそれぞれの機器内で生成できる。

制限認証対応の機器は共通の秘密情報と処理関数を持つ。認証時にはチャレンジ乱数を送信する。乱数を受け取った機器は所定の関数で処理し返送する。チャレンジ乱数を送信した機器は、応答と機器内で処理した値とを比較することにより、正しい機器であることを確認する。認証を行う二台の間で

のみ有効な認証鍵を、両方の乱数を用いてそれぞれの機器内で生成できる。

以上の認証処理により正しい機器であることを確認できると、送信機は、交換鍵を認証鍵で暗号化して受信機に送信する。これにより、受信機側ではコンテンツ鍵を得ることができ、受信したコンテンツの暗号を解いて利用することができる。

以下、図12を参照して、IEEE1394バスシステムについて説明する。

図12で、IEEE1394バス#1(50)と、IEEE1394バス#2(51)はそれぞれ異なったIEEE1394バスであり、ブリッジ装置52によって互いに接続されている。

IEEE1394バス#1(50)には、デバイス#0(53)、デバイス#1(54)などのデバイスが接続されている。

IEEE1394バス#2(51)には、デバイス#0(58)、デバイス#1(59)などのデバイスが接続されている。

デバイス#0(53)、デバイス#1(54)、デバイス#0(58)、デバイス#1(59)などは、IEEE1394バス#1(50)やIEEEバス#2(51)を利用してデータを送信または受信する機器であり、例えばSTB(セットトップボックス)やTV(テレビ)である。

また、ブリッジ装置52は、IEEE1394バス#1(54)に接続されたデバイス#2(55)などから送信されたデータを受信して、IEEE1394バス#2に送信する装置である。

IEEE1394の規格では、1つのバスに同時に最大63台までのデバイスを接続することが出来るという制限がある。従って、IEEE1394バス#1(50)には、同時に最大63台までのデバイスを接続することが出来、又IEEE1394バス#2(51)にも、同時に最大63台までのデバイスを接続することが出来る。

例えば図12の例では、IEEE1394バス#1(50)には、ブリッジ装置52も含めて7台のデバイスが接続されているので、あと56台接続することが出来る。

デバイス53は、20Mbpsの伝送レートでデータをアイソクロナス伝送と呼ばれる同期転送によりIEEE1394バス#1(50)の1チャンネルに送信している。そして、デバイス#1(54)は、IEEE1394バス#1(50)の1チャンネルに転送されているデータを受信している。

また、デバイス#4(56)は、40Mbpsの伝送レートでデータをIEEE1394バス#1(50)の63チャンネルに送信している。そして、デバイス#5(57)は63チャンネルで伝送されているデータを受信している。

同様にIEEE1394バス#2(51)では、デバイス#0(58)が、2チャンネルに30Mbpsの伝送レートでデータを送信し、2チャンネルに伝送されているデータをデバイス#1(59)が受信している。また、デバイス#3(61)が30Mbpsのデータを1チャンネルに送信しており、1チャンネルに伝送されているデータをデバイス#4(62)と、デバイス#5(63)が同時に受信している。

一方、デバイス#2(55)は、IEEE1394バス#1(50)の0チャンネルに20Mbpsの伝送レートでデータを送信している。ブリッジ52は、IEEE1394バス#1(50)の0チャンネルに伝送されているデータを受信し、IEEE1394バス#2(51)の0チャンネルに送信している。そして、デバイス#2(60)は、IEEE1394バス#2(51)の0チャンネルに伝送されているデータを受信している。

このように、アイソクロナス伝送を使用してリアルタイムにデータを伝送することが可能であり、また、2つの異なったIEEE1394バスをブリッジ装置52で接続すると、デバイスが送信したデータをブリッジ装置を経

由して異なったバスに接続されたデバイスがリアルタイムに受信することが出来る。

ところで、著作権者からは、著作権保護が必要な映像音声データ（AVデータ）などを送信する際、信号源となる機器からの信号を受けとることが出来る受信機器の数を制限したいという要望がある。

前述したように、1つのIEEE1394バスには同時に最大63台しか機器が接続出来ないという制限がある。従って信号源となる機器から送信されたデータを同時に受信出来る受信機器の数は最大でも62台である。

ところが、上記のように異なったIEEE1394バスをブリッジ装置で接続すると、信号源となる機器に対してブリッジ装置52を介した他方のバスで何台の受信機器に信号源となる機器からの信号が受信されるかが、把握出来なくなる。例えば、信号源となる機器に対してブリッジ装置52を介した他方のバスにさらにブリッジ装置が接続されている場合などが起こりうる。このように、ブリッジ装置52がIEEE1394バスに接続されると、非常に多数の受信機器に信号源となる機器から送信された信号が受け取られる危険性がある。また、IEEE1394バスに限らず、USBなどのネットワークの場合でも同様のことが言える。

すなわち、IEEE1394バスなどのネットワークにブリッジ装置が接続されると、非常に多数の受信機器に信号源となる機器から送信された著作権保護が必要な信号が受信される危険性があり、信号を受け取られる機器の数を制限したいという著作権者の要望を守ることが出来ないという課題（第1の課題）がある。

また、IEEE1394バスにブリッジ装置が接続されていない場合であっても、著作権者が5台までの受信機器にしか信号を受け取られたくないと希望しても、IEEE1394バスに同時に6台以上の受信機器を接続すると、著作権者の要望が守られなくなる。また、このことはIEEE1394

バスに限らず、USBなどのネットワークでも同様のことが言える。

すなわち、著作権者が信号を受け取ることが出来る受信機器の台数を指定して制限したいと要望しても、その要望を守ることが出来ないという課題（第2の課題）がある。

発明の開示

本発明は、上記第1の課題を考慮し、ネットワークにブリッジ装置が接続されていても、著作権保護が必要な信号を受け取ることが出来る受信機器の数を制限したいという著作権者の要望を守ることが出来る著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラムを提供することを目的とするものである。

また、本発明は、上記第2の課題を考慮し、著作権保護が必要な信号を受け取ることが出来る受信機器の数を受信機器の台数を指定して制限するという著作権者の要望を守ることが出来る著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラムを提供することを目的とするものである。

上述した課題を解決するために、第1の本発明（請求項1に対応）は、ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも1台以上の受信装置と、

前記受信装置に、前記ネットワークを利用して前記著作権保護が必要なデータを送信する送信装置とを備えた著作権保護システムであって、

前記送信装置は、前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記受信装置は、前記送信側認証手段と認証を行う受信側認証手段を有し

前記認証数に制限を設けたことを特徴とする著作権保護システムである。

また、第2の本発明（請求項2に対応）は、前記認証数カウント手段は、前記送信側認証手段が認証を行い成功すると、前記認証数を加算することを特徴とする第1の本発明の著作権保護システムである。

また、第3の本発明（請求項3に対応）は、前記受信装置は、前記送信装置と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度認証要求しないことを特徴とする第2の本発明の著作権保護システムである。

また、第4の本発明（請求項4に対応）は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置は、再度認証要求することが出来ることを特徴とする第3の本発明の著作権保護システムである。

また、第5の本発明（請求項5に対応）は、前記送信装置は、前記受信装置と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度前記受信装置から認証要求があってもその認証要求を受け付けないことを特徴とする第2の本発明の著作権保護システムである。

また、第6の本発明（請求項6に対応）は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置は、前記ブリッジ装置から認証要求が行われた場合、その認証要求を受け付けることを特徴とする第5の本発明の著作権保護システムである。

また、第7の本発明（請求項7に対応）は、前記送信装置は、前記受信装置と認証を行い成功した場合、再度前記受信装置と認証を行うが、所定の原因によって前記認証がリセットされない限り、たとえその認証に成功しても前記認証数カウント手段は、前記認証数を加算しないことを特徴とする第2の本発明の著作権保護システムである。

また、第8の本発明（請求項8に対応）は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記認証数カウント手段は、再度前記ブリッジ装置と認証を行い成功した場合、前記認証数を加算することを特徴とする第7の本発明の著作権保護システムである。

また、第9の本発明（請求項9に対応）は、前記送信側認証手段は、前記受信装置と認証を行い成功した場合、前記受信装置を特定する情報を登録する登録手段と、

前記受信装置から認証要求が行われると、その認証要求がすでに認証を行い成功した前記受信装置からの認証要求かどうかを登録した前記受信装置を特定する情報を利用して行う重複判定手段とを有することを特徴とする第3～8の本発明のいずれかの著作権保護システムである。

また、第10の本発明（請求項10に対応）は、前記認証のリセットは、鍵の更新が行われた時に起こることを特徴とする第3～8の本発明のいずれかの著作権保護システムである。

また、第11の本発明（請求項11に対応）は、前記認証のリセットは、交換鍵の更新が行われた時に起こることを特徴とする第3～8の本発明のいずれかの著作権保護システムである。

また、第12の本発明（請求項12に対応）は、前記ネットワークを他の

ネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置が前記鍵の更新を行った場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第10の本発明の著作権保護システムである。

また、第13の本発明（請求項13に対応）は、前記認証のリセットは、バスリセットされた際に起こることを特徴とする第3～8の本発明のいずれかの著作権保護システムである。

また、第14の本発明（請求項14に対応）は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置が接続されている前記ネットワークで、前記バスリセットされた場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第13の本発明の著作権保護システムである。

また、第15の本発明（請求項15に対応）は、前記認証数に制限を設けるとは、前記認証数が所定の値以上になった場合、前記送信側認証手段は、前記受信装置からの認証要求を受け付けないことであることを特徴とする第1の本発明の著作権保護システムである。

また、第16の本発明（請求項16に対応）は、前記送信側認証手段と認証を行い成功した前記受信装置が、前記送信装置から送られてくる前記著作権保護が必要なデータの使用中を中止した場合、前記認証数カウント手段は、前記認証数を減算することを特徴とする第1の本発明の著作権保護システムである。

また、第17の本発明（請求項17に対応）は、前記ネットワークを他の

ネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用中止するとは、前記他のネットワークに接続されているすべての前記受信装置が前記送信装置から送られてくる前記著作権の保護が必要なデータの使用中止したことであることを特徴とする第16の本発明の著作権保護システムである。

また、第18の本発明（請求項18に対応）は、前記送信装置は、前記送信側認証手段と認証を行い成功した前記受信装置を特定する情報を登録する登録手段を有し、

前記認証数カウント手段が前記認証数を減算した場合、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録を解除することを特徴とする第16の本発明の著作権保護システムである。

また、第19の本発明（請求項19に対応）は、前記送信装置は、前記受信装置が、前記著作権保護が必要なデータの使用中止したかどうかを調査する調査手段を有することを特徴とする第16の本発明の著作権保護システムである。

また、第20の本発明（請求項20に対応）は、前記著作権保護が必要なデータの使用中止するとは、前記受信装置が前記ネットワークから切り離されることであり、

前記調査手段は、前記受信装置が前記ネットワークから切り離されたかどうかを定期的に調査することを特徴とする第19の本発明の著作権保護システムである。

また、第21の本発明（請求項21に対応）は、前記調査するとは、前記ネットワークに接続されている前記受信装置の数である接続数を定期的に調

査し、前記接続数が減少した場合、どの前記受信装置が前記ネットワークから切り離されたかをチェックすることであることを特徴とする第20の本発明の著作権保護システムである。

また、第22の本発明（請求項22に対応）は、前記調査手段は、前記受信装置の動作状態及び／または接続プラグのアクティブ状態を調べることによって、前記受信装置が前記著作権保護が必要なデータの使用中を中止したかをチェックし、

前記認証数カウント手段は、前記調査手段の調査の結果、前記受信装置が前記著作権保護が必要なデータを使用していないようであれば、前記認証数を減算することを特徴とする第19の本発明の著作権保護システムである。

また、第23の本発明（請求項23に対応）は、前記調査手段は、前記受信装置を特定する情報と、その受信装置の署名とを対応付ける対応表を有し、

前記調査手段は、前記対応表を利用して、前記ネットワークから切り離された前記受信装置が認証済みであったかどうかを判定し、

前記認証数カウント手段は、前記判定結果が、前記ネットワークから切り離された前記受信装置が認証済みであったことを示す場合、前記認証数を減算することを特徴とする第20または21の本発明の著作権保護システムである。

また、第24の本発明（請求項24に対応）は、前記受信側認証手段は、前記受信装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用中を中止する場合、前記送信装置に前記認証数を減算するためのデクレメント認証要求を行い、

前記送信側認証手段は、前記受信側認証手段と、前記デクレメント認証を行い、

前記認証数カウント手段は、前記デクレメント認証が成功すると、前記認

証数を減算することを特報とする第 16 の本発明の著作権保護システムである。

また、第 25 の本発明（請求項 25 に対応）は、前記デクレメント認証を行うためのコマンドであるデクレメント認証用コマンドが、前記著作権保護が必要なデータを使用する際の認証を行うためのコマンドである認証コマンドとは別に作成されていることを特徴とする第 24 の本発明の著作権保護システムである。

また、第 26 の本発明（請求項 26 に対応）は、前記著作権保護が必要なデータは暗号化されており、

前記デクレメント認証が成功すると、前記受信装置は、前記著作権保護が必要なデータを解読するための鍵を放棄することを特徴とする第 24 または 25 の本発明の著作権保護システムである。

また、第 27 の本発明（請求項 27 に対応）は、前記デクレメント認証は、前記著作権保護が必要なデータを使用するための認証とは、署名、認証方法、演算式の少なくとも 1 つ以上が異なっていることを特徴とする第 24 または 25 の本発明の著作権保護システムである。

また、第 28 の本発明（請求項 28 に対応）は、所定の原因によって認証がリセットされた場合、前記認証数カウント手段は、前記認証数を初期化し、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録をすべて解除することを特徴とする第 18 の本発明の著作権保護システムである。

また、第 29 の本発明（請求項 29 に対応）は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられていることを特徴とする第 2 の本発明の著作権保護システムである。

また、第 30 の本発明（請求項 30 に対応）は、前記ブリッジ装置は、前記他のネットワークでは、前記送信装置として扱われ、

前記他のネットワークに接続された前記受信装置から認証要求が行われた場合、

その受信装置と認証を行う前に、前記ネットワークに接続された前記送信装置と認証を行い、その送信装置との認証が成功した場合、前記受信装置と認証を行うことを特徴とする第29の本発明の著作権保護システムである。

また、第31の本発明（請求項31に対応）は、前記ブリッジ装置の前記認証数カウント手段が減算された場合、前記ブリッジ装置は、前記ネットワークに接続された前記送信装置と、前記ネットワークに接続された前記送信装置の前記認証数カウント手段がカウントしている前記認証数を減算させるためのデクレメント認証を行うことを特徴とする第29の本発明の著作権保護システムである。

また、第32の本発明（請求項32に対応）は、前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である認証数をカウントすることを特徴とする第29の本発明の著作権保護システムである。

また、第33の本発明（請求項33に対応）は、前記ネットワークに新たに前記送信装置が接続された場合、前記ブリッジ装置は、前記ブリッジ装置の前記認証数カウント手段がカウントしていた前記認証数の回数だけ新たに接続された前記送信装置と認証を行うことを特徴とする第32の本発明の著作権保護システムである。

また、第34の本発明（請求項34に対応）は、前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を有し、

前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を

行い成功した数である前記認証数をカウントし、

前記ブリッジ装置は、前記ネットワークに接続された前記送信装置と認証して成功した数を前記鍵カウンタがカウントしている前記許可の限度数とし

、
前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数を減算するためのデクレメント認証要求があった場合、前記ブリッジ装置は前記ネットワークに接続されている前記送信装置とデクレメント認証を行わず、その受信装置とデクレメント認証を行い、

前記デクレメント認証が成功すると、前記ブリッジ装置の前記認証数カウント手段は、前記認証数を減算し、

前記他のネットワークに接続されている前記受信装置から新たに認証要求があった際、

前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より小さい場合には、その受信装置と認証を行い、

前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より小さくない場合には、その受信装置と認証を行う前に前記ネットワークに接続されている前記送信装置と認証を行い、その認証が成功した場合、その受信装置と認証を行うことを特徴とする第30の本発明の著作権保護システムである。

また、第35の本発明（請求項35に対応）は、前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から送られてくるデータを再暗号化して、前記他のネットワークに接続されている前記受信装置に送信し

、
前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を

行い成功した数である認証数をカウントし、

前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を有することを特徴とする第 29 の本発明の著作権保護システムである。

また、第 36 の本発明（請求項 36 に対応）は、前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数と前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きい場合、その認証要求を許可することを特徴とする第 35 の本発明の著作権保護システムである。

また、第 37 の本発明（請求項 37 に対応）は、前記鍵カウント手段がカウントしている許可の限度数の上限は予め前記ネットワークに接続されている前記送信装置から与えられていることを特徴とする第 36 の本発明の著作権保護システムである。

また、第 38 の本発明（請求項 38 に対応）は、前記鍵カウント手段がカウントしている許可の限度数の上限は、前記ブリッジ装置が前記ネットワークに接続されている前記送信装置と認証を行うことによって、加算されることを特徴とする第 36 の本発明の著作権保護システムである。

また、第 39 の本発明（請求項 39 に対応）は、前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、その認証要求を拒絶することを特徴とする第 35 の本発明の著作権保護システムである。

また、第 40 の本発明（請求項 40 に対応）は、前記ブリッジ装置は、前

記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ネットワークに接続されている前記送信装置に前記許可の限度数を加算するよう依頼することを特徴とする第 35 の本発明の著作権保護システムである。

また、第 4 1 の本発明（請求項 4 1 に対応）は、前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ネットワークに接続されている前記送信装置に認証要求を行い、前記認証が成功した場合、前記鍵カウント手段は、前記許可の限度数を加算することを特徴とする第 35 の本発明の著作権保護システムである。

また、第 4 2 の本発明（請求項 4 2 に対応）は、前記ブリッジ装置は、前記他のネットワークに接続された前記受信装置から認証要求される毎に、前記ネットワークに接続された前記送信装置に前記他のネットワークに接続された前記受信装置のうち認証要求を行っているものの台数を通知することを特徴とする第 29 の本発明の著作権保護システムである。

また、第 4 3 の本発明（請求項 4 3 に対応）は、前記ブリッジ装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドには、前記台数を通知するためのフィールドが設けられており、前記ブリッジ装置は、前記フィールドを利用して前記台数の通知を行うことを特徴とする第 4 2 の本発明の著作権保護システムである。

また、第 4 4 の本発明（請求項 4 4 に対応）は、前記ブリッジ装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドは、前記ブリッジ装置の機能を有しない前記ネットワークに接続さ

れた前記受信装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドとは区別されていることを特徴とする第 29 の本発明の著作権保護システムである。

また、第 45 の本発明（請求項 45 に対応）は、前記区別は、前記認証コマンドに添付する署名によって行われることを特徴とする第 44 の本発明の著作権保護システムである。

また、第 46 の本発明（請求項 46 に対応）は、送信装置と認証する受信側認証手段を有し、ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも 1 台以上の受信装置に対して、前記ネットワークを利用して前記著作権保護が必要なデータを送信する送信装置であって、
前記受信側認証手段と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記認証数に制限を設けたことを特徴とする送信装置である。

また、第 47 の本発明（請求項 47 に対応）は、ネットワークに接続され、著作権保護が必要なデータを受信して使用する受信装置であって、

前記受信装置と認証を行う送信側認証手段と、前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有する送信装置の前記送信側認証手段と認証する受信側認証手段を備え、

前記認証数に制限を設けたことを特徴とする受信装置である。

また、第 48 の本発明（請求項 48 に対応）は、前記一方のネットワークに接続された送信装置から送信された著作権保護が必要なデータを前記他のネットワークに接続された受信装置に送信するブリッジ装置であって、

前記受信装置と認証を行うブリッジ装置用送信側認証手段と、

前記送信側認証手段が認証した数であるブリッジ装置用認証数を数えるブリッジ装置用認証数カウント手段と、

前記送信装置と認証を行うブリッジ装置用受信側認証手段とを備え、
前記送信装置は、前記ブリッジ装置または前記ネットワークに接続された
前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手
段とを有し、

前記受信装置は、前記ブリッジ装置または前記他のネットワークに接続さ
れた前記送信装置と認証する受信側認証手段を有し、

前記送信側認証手段が数える前記認証数に制限を設けたことを特徴とする
ブリッジ装置である。

また、第49の本発明（請求項49に対応）は、ネットワークに接続され
、著作権保護が必要なデータを受信して使用する少なくとも一台以上の受信
装置に、前記ネットワークを利用して送信装置から前記著作権保護が必要な
データを送信する著作権保護方法であって、

前記送信装置は、前記受信装置と認証した数である認証数を数え、
前記認証数に制限を設けたことを特徴とする著作権保護方法である。

また、第50の本発明（請求項50に対応）は、第1の本発明の著作権保
護システムの、前記受信装置における、前記送信側認証手段と認証を行う受
信側認証手段と、

前記送信装置における、前記受信装置と認証を行う送信側認証手段と、
前記送信側認証手段が認証した数である認証数を数える認証数カウント手
段との全部または一部としてコンピュータを機能させるためのプログラ
ムを担持した媒体であって、コンピュータにより処理可能である媒体で
ある。

また、第51の本発明（請求項51に対応）は、第1の本発明の著作権保
護システムの、前記受信装置における、前記送信側認証手段と認証を行う受
信側認証手段と、

前記送信装置における、前記受信装置と認証を行う送信側認証手段と、
前記送信側認証手段が認証した数である認証数を数える認証数カウント手段との全部または一部としてコンピュータを機能させるためのプログラムである。

なお、第1の他の発明は、前記認証数カウント手段は、前記送信側認証手段が認証を行い成功すると、前記認証数を加算することを特徴とする第46の本発明の送信装置である。本発明は、第1の他の発明であってもよい。

また、第2の他の発明は、前記受信装置は、前記送信側認証手段と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度認証要求しないことを特徴とする第46の本発明の送信装置である。本発明は、第2の他の発明であってもよい。

また、第3の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置は、再度認証要求することが出来ることを特徴とする第2の他の発明の送信装置である。本発明は、第3の他の発明であってもよい。

また、第4の他の発明は、前記送信側認証手段は、前記受信装置と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度前記受信装置から認証要求があってもその認証要求を受け付けないことを特徴とする第1の他の発明の送信装置である。本発明は、第4の他の発明であってもよい。

また、第5の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信側認証手段は、前記ブリッジ装置から認証要求が行われた場合、その認証要求を受け付けることを特徴とする第４の他の発明の送信装置である。本発明は、第５の他の発明であってもよい。

また、第６の他の発明は、前記送信側認証手段は、前記受信装置と認証を行い成功した場合、再度前記受信装置と認証を行うが、所定の原因によって前記認証がリセットされない限り、たとえその認証に成功しても前記認証数カウント手段は、前記認証数を加算しないことを特徴とする第１の他の発明の送信装置である。本発明は第６の他の発明であってもよい。

また、第７の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記認証数カウント手段は、再度前記ブリッジ装置と認証を行い成功した場合、前記認証数を加算することを特徴とする第６の他の発明の送信装置である。本発明は、第７の他の発明であってもよい。

また、第８の他の発明は、前記送信側認証手段は、前記受信装置と認証を行い成功した場合、前記受信装置を特定する情報を登録する登録手段と、

前記受信装置から認証要求が行われると、その認証要求がすでに認証を行い成功した前記受信装置からの認証要求かどうかを登録した前記受信装置を特定する情報を利用して行う重複判定手段とを有することを特徴とする第２～７の他の発明のいずれかの送信装置である。本発明は、第８の他の発明であってもよい。

また、第９の他の発明は、前記認証のリセットは、鍵の更新が行われた時に起こることを特徴とする第２～７の他の発明のいずれかに記載の送信装置である。本発明は、第９の他の発明であってもよい。

また、第１０の他の発明は、前記認証のリセットは、交換鍵の更新が行わ

れた時に起こることを特徴とする第 2～7 の他の発明のいずれかの送信装置である。本発明は第 10 の他の発明であってもよい。

また、第 11 の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信側認証手段が前記鍵の更新を行った場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第 9 の他の発明の送信装置である。本発明は、第 11 の他の発明であってもよい。

また、第 12 の他の発明は、前記認証のリセットは、バスリセットされた際に起こることを特徴とする第 2～7 の他の発明のいずれかの送信装置である。本発明は、第 12 の他の発明であってもよい。

また、第 13 の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

送信装置が接続されている前記ネットワークで、前記バスリセットされた場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第 12 の他の発明の送信装置である。本発明は、第 13 の他の発明であってもよい。

また、第 14 の他の発明は、前記認証数に制限を設けるとは、前記認証数が所定の値以上になった場合、前記送信側認証手段は、前記受信装置からの認証要求を受け付けないことであることを特徴とする第 46 の本発明の送信装置である。本発明は、第 14 の他の発明であってもよい。

また、第 15 の他の発明は、前記送信側認証手段と認証を行い成功した前記受信装置が、送信装置から送られてくる前記著作権保護が必要なデータの

使用を中止した場合、前記認証数カウント手段は、前記認証数を減算することを特徴とする第４６の本発明の送信装置である。本発明は、第１５の他の発明であってもよい。

また、第１６の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置が送信装置から送られてくる前記著作権保護が必要なデータの使用を中止するとは、前記他のネットワークに接続されているすべての前記受信装置が送信装置から送られてくる前記著作権の保護が必要なデータの使用を中止したことであることを特徴とする第１５の他の発明の送信装置である。本発明は、第１６の他の発明であってもよい。

また、第１７の他の発明は、前記送信側認証手段と認証を行い成功した前記受信装置を特定する情報を登録する登録手段を備え、

前記認証数カウント手段が前記認証数を減算した場合、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録を解除することを特徴とする第１５の他の発明の送信装置である。本発明は第１７の他の発明であってもよい。

また、第１８の他の発明は、前記受信装置が、前記著作権保護が必要なデータの使用を中止したかどうかを調査する調査手段を備えたことを特徴とする第１５の他の発明の送信装置である。本発明は、第１８の他の発明であってもよい。

また、第１９の他の発明は、前記著作権保護が必要なデータの使用を中止するとは、前記受信装置が前記ネットワークから切り離されることであり、

前記調査手段は、前記受信装置が前記ネットワークから切り離されたかどうかを定期的に調査することを特徴とする第１８の他の発明の送信装置であ

る。本発明は、第 19 の他の発明であってもよい。

また、第 20 の他の発明は、前記調査するとは、前記ネットワークに接続されている前記受信装置の数である接続数を定期的に調査し、前記接続数が減少した場合、どの前記受信装置が前記ネットワークから切り離されたかをチェックすることであることを特徴とする第 19 の他の発明の送信装置である。本発明は、第 20 の他の発明であってもよい。

また、第 21 の他の発明は、前記調査手段は、前記受信装置の動作状態及び／または接続プラグのアクティブ状態を調べることによって、前記受信装置が前記著作権保護が必要なデータの使用を中止したかをチェックし、

前記認証数カウント手段は、前記調査手段の調査の結果、前記受信装置が前記著作権保護が必要なデータを使用していないようであれば、前記認証数を減算することであることを特徴とする第 18 の他の発明の送信装置である。本発明は、第 21 の他の発明であってもよい。

また、第 22 の他の発明は、前記調査手段は、前記受信装置を特定する情報と、その受信装置の署名とを対応付ける対応表を有し、

前記調査手段は、前記対応表を利用して、前記ネットワークから切り離された前記受信装置が認証済みであったかどうかを判定し、

前記認証数カウント手段は、前記判定結果が、前記ネットワークからきりはなされた前記受信装置が認証済みであったことを示す場合、前記認証数を減算することであることを特徴とする第 19 または 20 の他の発明の送信装置である。本発明は、第 22 の他の発明であってもよい。

また、第 23 の他の発明は、前記受信側認証手段は、前記受信装置が送信装置から送られてくる前記著作権保護が必要なデータの使用を中止する場合、前記送信側認証手段に前記認証数を減算するためのデクレメント認証要求を行い、

前記送信側認証手段は、前記受信側認証手段と、前記デクレメント認証を

行い、

前記認証数カウント手段は、前記デクレメント認証が成功すると、前記認証数を減算することを特報とする第15の他の発明の送信装置である。本発明は、第23の他の発明であってもよい。

また、第24の他の発明は、前記デクレメント認証を行うためのコマンドであるデクレメント認証用コマンドが、前記著作権保護が必要なデータを使用する際の認証を行うためのコマンドである認証コマンドとは別に作成されていることを特徴とする第23の他の発明の送信装置である。本発明は、第24の他の発明であってもよい。

また、第25の他の発明は、前記著作権保護が必要なデータは暗号化されており、

前記デクレメント認証が成功すると、前記受信装置は、前記著作権保護が必要なデータを解読するための鍵を放棄することを特徴とする第23または24の他の発明の送信装置である。本発明は、第25の他の発明であってもよい。

また、第26の他の発明は、前記デクレメント認証は、前記著作権保護が必要なデータを使用するための認証とは、署名、認証方法、演算式の少なくとも1つ以上が異なっていることを特徴とする第23または24の他の発明の送信装置である。本発明は、第26の他の発明であってもよい。

また、第27の他の発明は、所定の原因によって認証がリセットされた場合、前記認証数カウント手段は、前記認証数を初期化し、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録をすべて解除することを特徴とする第17の他の発明の送信装置である。本発明は、第27の他の発明であってもよい。

また、第28の他の発明は、前記認証数カウント手段は、前記送信側認証手段が認証を行い成功すると、前記認証数を加算することを特徴とする第4

7の本発明の受信装置である。本発明は、第28の他の発明であってもよい。

また、第29の他の発明は、前記受信側認証手段は、前記送信装置と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度認証要求しないことを特徴とする第28の他の発明の受信装置である。本発明は、第29の他の発明であってもよい。

また、第30の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記ブリッジ装置は、再度認証要求することが出来ることを特徴とする第29の他の発明の受信装置である。本発明は、第30の他の発明であってもよい。

また、第31の他の発明は、前記送信装置は、前記受信側認証手段と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度前記受信側認証手段から認証要求があってもその認証要求を受け付けないことを特徴とする第28の他の発明の受信装置である。本発明は、第31の他の発明であってもよい。

また、第32の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置であり、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記送信装置は、前記ブリッジ装置から認証要求が行われた場合、その認証要求を受け付けることを特徴とする第31の他の発明の受信装置である。本発明は、第32の他の発明であってもよい。

また、第33の他の発明は、前記送信装置は、前記受信側認証手段と認証を行い成功した場合、再度前記受信側認証手段と認証を行うが、所定の原因

によって前記認証がリセットされない限り、たとえその認証に成功しても前記認証数カウント手段は、前記認証数を加算しないことを特徴とする第28の他の発明の受信装置である。本発明は、第33の他の発明であってもよい。

また、第34の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置であり、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記認証数カウント手段は、再度前記ブリッジ装置と認証を行い成功した場合、前記認証数を加算することを特徴とする第33の他の発明の受信装置である。本発明は、第34の他の発明であってもよい。

また、第35の他の発明は、前記送信側認証手段は、前記受信側認証手段と認証を行い成功した場合、前記受信側認証手段を特定する情報を登録する登録手段と、

前記受信側認証手段から認証要求が行われると、その認証要求がすでに認証を行い成功した前記受信側認証手段からの認証要求かどうかを登録した前記受信側認証手段を特定する情報を利用して行う重複判定手段とを有することを特徴とする第29～34の他の発明のいずれかの受信装置である。本発明は、第35の他の発明であってもよい。

また、第36の他の発明は、前記認証のリセットは、鍵の更新が行われた時に起こることを特徴とする第29～34の他の発明のいずれかの受信装置である。本発明は、第36の他の発明であってもよい。

また、第37の他の発明は、前記認証のリセットは、交換鍵の更新が行われた時に起こることを特徴とする第29～34の他の発明のいずれかの受信装置である。本発明は、第37の他の発明であってもよい。

また、第38の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置であり、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記送信装置が前記鍵の更新を行った場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第 36 の他の発明の受信装置である。本発明は、第 38 の他の発明であってもよい。

また、第 39 の他の発明は、前記認証のリセットは、バスリセットされた際に起こることを特徴とする第 29～34 の他の発明のいずれかの受信装置である。本発明は、第 39 の他の発明であってもよい。

また、第 40 の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置であり、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記送信装置が接続されている前記ネットワークで、前記バスリセットされた場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第 39 の他の発明の受信装置である。本発明は、第 40 の他の発明であってもよい。

また、第 41 の他の発明は、前記認証数に制限を設けるとは、前記認証数が所定の値以上になった場合、前記送信側認証手段は、前記受信側認証手段からの認証要求を受け付けないことであることを特徴とする第 47 の本発明の受信装置である。本発明は、第 41 の他の発明であってもよい。

また、第 42 の他の発明は、前記送信側認証手段と認証を行い成功した前記受信側認証手段が、前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止した場合、前記認証数カウント手段は、前記認証数を減算することを特徴とする第 47 の本発明の受信装置である。本発明は、第 42 の他の発明であってもよい。

また、第 43 の他の発明は、前記ネットワークを他のネットワークに接続

するためのブリッジ装置であり、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記ブリッジ装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用中止するとは、前記他のネットワークに接続されているすべての受信装置が前記送信装置から送られてくる前記著作権の保護が必要なデータの使用中止したことを特徴とする第４２の他の発明の受信装置である。本発明は、第４３の他の発明であってもよい。

また、第４４の他の発明は、前記送信装置は、前記送信側認証手段と認証を行い成功した前記受信側認証手段を特定する情報を登録する登録手段を有し、

前記認証数カウント手段が前記認証数を減算した場合、前記登録手段は、前記送信側認証手段と認証を行い成功した前記受信側認証手段を特定する情報の登録を解除することを特徴とする第４２の他の発明の受信装置である。本発明は、第４４の他の発明であってもよい。

また、第４５の他の発明は、前記送信装置は、受信装置が、前記著作権保護が必要なデータの使用中止したかどうかを調査する調査手段を有することを特徴とする第４２の他の発明の受信装置である。本発明は、第４５の他の発明であってもよい。

また、第４６の他の発明は、前記著作権保護が必要なデータの使用中止するとは、受信装置が前記ネットワークから切り離されることであり、

前記調査手段は、前記受信装置が前記ネットワークから切り離されたかどうかを定期的に調査することを特徴とする第４５の他の発明の受信装置である。本発明は、第４６の他の発明であってもよい。

また、第４７の他の発明は、前記調査するとは、前記ネットワークに接続されている受信装置の数である接続数を定期的に調査し、前記接続数が減少

した場合、どの受信装置が前記ネットワークから切り離されたかをチェックすることであることを特徴とする第４６の他の発明の受信装置である。本発明は、第４７の他の発明であってもよい。

また、第４８の他の発明は、前記調査手段は、前記受信装置の動作状態及び／または接続プラグのアクティブ状態を調べることによって、受信装置が前記著作権保護が必要なデータの使用を中止したかをチェックし、

前記認証数カウント手段は、前記調査手段の調査の結果、前記受信装置が前記著作権保護が必要なデータを使用していないようであれば、前記認証数を減算することを特徴とする第４５の他の発明の受信装置である。本発明は、第４８の他の発明であってもよい。

また、第４９の他の発明は、前記調査手段は、受信装置を特定する情報と、その受信装置の署名とを対応付ける対応表を有し、

前記調査手段は、前記対応表を利用して、前記ネットワークから切り離された前記受信装置が認証済みであったかどうかを判定し、

前記認証数カウント手段は、前記判定結果が、前記ネットワークからきりはなされた前記受信装置が認証済みであったことを示す場合、前記認証数を減算することを特徴とする第４６または４７の他の発明の受信装置である。本発明は、第４９の他の発明であってもよい。

また、第５０の他の発明は、前記受信側認証手段は、受信装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止する場合、前記送信装置に前記認証数を減算するためのデクレメント認証要求を行い、

前記送信側認証手段は、前記受信側認証手段と、前記デクレメント認証を行い、

前記認証数カウント手段は、前記デクレメント認証が成功すると、前記認証数を減算することを特報とする第４２の他の発明の受信装置である。本発

明は、第50の他の発明であってもよい。

また、第51の他の発明は、前記デクレメント認証を行うためのコマンドであるデクレメント認証用コマンドが、前記著作権保護が必要なデータを使用する際の認証を行うためのコマンドである認証コマンドとは別に作成されていることを特徴とする第50の他の発明の受信装置である。本発明は、第51の他の発明であってもよい。

また、第52の他の発明は、前記著作権保護が必要なデータは暗号化されており、

前記デクレメント認証が成功すると、受信装置は、前記著作権保護が必要なデータを解読するための鍵を放棄することを特徴とする第50または51の他の発明の受信装置である。本発明は、第52の他の発明であってもよい。

また、第53の他の発明は、前記デクレメント認証は、前記著作権保護が必要なデータを使用するための認証とは、署名、認証方法、演算式の少なくとも1つ以上が異なっていることを特徴とする第50または51の他の発明の受信装置である。本発明は、第53の他の発明であってもよい。

また、第54の他の発明は、所定の原因によって認証がリセットされた場合、前記認証数カウント手段は、前記認証数を初期化し、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録をすべて解除することを特徴とする第44の他の発明の受信装置。本発明は、第54の他の発明であってもよい。

また、第55の他の発明は、前記他のネットワークでは、前記送信装置として扱われ、

前記他のネットワークに接続された前記受信装置から認証要求が行われた場合、

前記ブリッジ装置用送信側認証手段が、その受信装置と認証を行う前に、前記ブリッジ装置用受信側認証手段が、前記ネットワークに接続された前記

送信装置と認証を行い、その送信装置との認証が成功した場合、前記ブリッジ装置用送信側認証手段は、前記受信装置と認証を行うことを特徴とする第48の本発明のブリッジ装置である。本発明は、第55の他の発明であつてもよい。

また、第56の他の発明は、前記ブリッジ装置用認証数カウント手段が減算された場合、前記ブリッジ装置用受信側認証手段は、前記ネットワークに接続された前記送信装置と、前記ネットワークに接続された前記送信装置の前記認証数カウント手段がカウントしている前記認証数を減算させるためのデクレメント認証を行うことを特徴とする第48の本発明のブリッジ装置である。本発明は、第56の他の発明であつてもよい。

また、第57の他の発明は、前記ブリッジ装置用認証数カウント手段は、前記ブリッジ装置用送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である認証数をカウントすることを特徴とする第48の本発明のブリッジ装置である。本発明は、第57の他の発明であつてもよい。

また、第58の他の発明は、前記ネットワークに新たに前記送信装置が接続された場合、前記ブリッジ装置用受信側認証手段は、前記ブリッジ装置用認証数カウント手段がカウントしていた前記認証数の回数だけ新たに接続された前記送信装置と認証を行うことを特徴とする第57の他の発明のブリッジ装置。本発明は、第58の他の発明であつてもよい。

また、第59の他の発明は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を備え、

前記ブリッジ装置用認証数カウント手段は、前記ブリッジ装置用送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である前記認証数をカウントし、

前記ネットワークに接続された前記送信装置と認証して成功した数を前記鍵カウンタがカウントしている前記許可の限度数とし、

前記他のネットワークに接続されている前記受信装置から前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数を減算するためのデクレメント認証要求があった場合、前記ブリッジ装置用受信側認証手段は前記ネットワークに接続されている前記送信装置とデクレメント認証を行わず、前記ブリッジ装置用送信側認証手段がその受信装置とデクレメント認証を行い、

前記デクレメント認証が成功すると、前記ブリッジ装置用認証数カウント手段は、前記認証数を減算し、

前記他のネットワークに接続されている前記受信装置から新たに認証要求があった際、

前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より小さい場合には、前記ブリッジ装置用送信側認証手段は、その受信装置と認証を行い、

前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より小さくない場合には、その受信装置と認証を行う前に前記ブリッジ装置用受信側認証手段が前記ネットワークに接続されている前記送信装置と認証を行い、その認証が成功した場合、前記ブリッジ装置用送信側認証手段がその受信装置と認証を行うことを特徴とする第55の他の発明のブリッジ装置である。本発明は、第59の他の発明であってもよい。

また、第60の他の発明は、前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を備え、

前記ネットワークに接続されている前記送信装置から送られてくるデータを再暗号化して、前記他のネットワークに接続されている前記受信装置に送

信し、

前記ブリッジ装置用認証数カウント手段は、前記ブリッジ装置用送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である認証数をカウントする第48の本発明のブリッジ装置である。本発明は、第60の他の発明であってもよい。

また、第61の他の発明は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数と前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より大きい場合、その認証要求を許可することを特徴とする第60の他の発明のブリッジ装置である。本発明は、第61の他の発明であってもよい。

また、第62の他の発明は、前記鍵カウント手段がカウントしている許可の限度数の上限は予め前記ネットワークに接続されている前記送信装置から与えられていることを特徴とする第61の他の発明のブリッジ装置である。本発明は、第62の他の発明であってもよい。

また、第63の他の発明は、前記鍵カウント手段がカウントしている許可の限度数の上限は、前記ブリッジ装置用受信側認証手段が前記ネットワークに接続されている前記送信装置と認証を行うことによって、加算されることを特徴とする第61の他の発明のブリッジ装置である。本発明は、第63の他の発明であってもよい。

また、第64の他の発明は、前記ブリッジ装置用送信側認証手段は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より大きくない場合、その認証要求を拒絶することを特徴とする第60の他の発明のブリッジ

装置である。本発明は、第 6 4 の他の発明であってもよい。

また、第 6 5 の他の発明は、前記ブリッジ装置用送信側認証手段は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ネットワークに接続されている前記送信装置に前記許可の限度数を加算するよう依頼することを特徴とする第 6 0 の他の発明のブリッジ装置である。本発明は、第 6 5 の他の発明であってもよい。

また、第 6 6 の他の発明は、前記ブリッジ装置用送信側認証手段は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ブリッジ装置用受信側認証手段は、前記ネットワークに接続されている前記送信装置に認証要求を行い、前記認証が成功した場合、前記鍵カウント手段は、前記許可の限度数を加算することを特徴とする第 3 5 の他の発明のブリッジ装置である。本発明は、第 6 6 の他の発明であってもよい。

また、第 6 7 の他の発明は、前記ブリッジ装置用送信側認証手段が前記他のネットワークに接続された前記受信装置から認証要求される毎に、前記ブリッジ装置用受信側認証手段が前記ネットワークに接続された前記送信装置に前記他のネットワークに接続された前記受信装置のうち認証要求を行っているものの台数を通知することを特徴とする第 4 8 の本発明のブリッジ装置である。本発明は、第 6 7 の他の発明であってもよい。

また、第 6 8 の他の発明は、前記ブリッジ装置用受信側認証手段が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドには、前記台数を通知するためのフィールドが設けられており、前記ブリッジ装置用受信側認証手段は、前記フィールドを利用して前記台数の通

知を行うことを特徴とする第 6 7 の他の発明のブリッジ装置である。本発明は、第 6 8 の他の発明であってもよい。

また、第 6 9 の他の発明は、前記ブリッジ装置用受信側認証手段が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドは、前記ブリッジ装置の機能を有しない前記ネットワークに接続された前記受信装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドとは区別されていることを特徴とする第 4 8 の本発明のブリッジ装置である。本発明は、第 6 9 の他の発明であってもよい。

また、第 7 0 の他の発明は、前記区別は、前記認証コマンドに添付する署名によって行われることを特徴とする第 6 9 の他の発明のブリッジ装置である。本発明は、第 7 0 の他の発明であってもよい。

図面の簡単な説明

図 1 は、本発明の第 1 ～第 7 の実施の形態における著作権保護システムの構成を示す図である。

図 2 は、本発明の第 1 の実施の形態における S T B の構成を示す図である。

図 3 は、本発明の第 1、第 2、第 7、第 8 の実施の形態における T V 3 0 の構成を示す図である。

図 4 は、本発明の第 1 の実施の形態における認証数カウント手段がカウントしている認証数とデバイス情報格納手段が格納しているデバイス情報の例を示す図である。

図 5 は、本発明の第 2、第 7、第 8 の実施の形態における S T B 4 0 の構成を示す図である。

図 6 は、本発明の第 2 の実施の形態における認証数カウント手段がカウントしている認証数とデバイス情報格納手段が格納しているデバイス情報の例

を示す図である。

図 7 は、本発明の第 3 の実施の形態における S T B の構成を示す図である。

図 8 は、本発明の第 3 及び第 4 の実施の形態における T V の構成を示す図である。

図 9 は、本発明の第 4 の実施の形態における S T B の構成を示す図である。

図 10 は、本発明の第 5 の実施の形態におけるブリッジ装置の構成を示す図である。

図 11 は、本発明の第 5 の実施の形態におけるブリッジ装置の動作を説明するステートマシン図である。

図 12 は、従来のバスシステムの構成を示す図である。

符号の説明

- 1 I E E E 1 3 9 4 バス # 1
- 2 I E E E 1 3 9 4 バス # 2
- 3 ソース
- 4 シンク 0
- 5 シンク 1
- 6 シンク 2 (ブリッジ装置)
- 7 シンク 3
- 8 シンク 4
- 9 シンク 5
- 20 S T B
- 21 送信側 D - I / F
- 22 暗号化手段
- 23 送信側認証手段
- 24 認証数カウント手段

- 25 認証上限数格納手段
- 26 カウント調整・判定手段
- 27 デバイス情報格納手段
- 28 送信側認証選択手段
- 29 送信側認証ルール格納手段
- 30 TV
- 31 受信側D-I/F
- 32 復号手段
- 33 認証要求手段
- 34 受信側認証手段
- 35 受信側認証選択手段
- 36 受信側認証ルール格納手段

発明を実施するための最良の形態

以下に、本発明の実施の形態を図面を参照して説明する。

(第1の実施の形態)

まず、第1の実施の形態について説明する。

図1に、本実施の形態の著作権保護システムを示す。

本実施の形態の著作権保護システムは、IEEE1394バス#1(1)、IEEE1394バス#2(2)がシンク2(ブリッジ装置)(6)によって接続され、IEEE1394バス#1(1)には、ソース3、シンク0(4)などが接続されている。また、IEEE1394バス#2(2)には、シンク5(9)、シンク6(10)などが接続されている。

IEEE1394バス#1(1)とIEEE1394バス#2(2)は、それぞれ異なったIEEE1394バスである。

ソース3は、IEEE1304バス#1(1)に著作権保護が必要なAVデータを送信する機器であり、例えばSTB(セットトップボックス)である。

シンク0(4)、シンク1(5)、シンク3(9)、シンク4(8)は、IEEE1394バス#1(1)に接続されており、ソース3から送信された著作権保護が必要なAVデータを受信して使用する機器であり、例えばTV(テレビ)である。

シンク5(9)、シンク6(10)、シンク7(11)は、IEEE1394バス#2(2)に接続されており、IEEE1394バス#2(2)に伝送されている著作権保護が必要なAVデータを受信して使用する機器であり、例えばTV(テレビ)である。

ブリッジ装置6は、ソース3から送信された著作権保護が必要なAVデータを受信して、再暗号化してから送信する装置である。ブリッジ装置6がAVデータの伝送を中継するので、IEEE1394バス#1(1)に接続されたソース3から送信された著作権保護が必要なAVデータを、IEEE1394バス#2(2)に接続されたシンク5(9)などが受信することが出来る。

図2に、ソース3の構成を示す。図2では、ソース3をSTB20として示した。

STB20は、送信側D-I/F21、暗号化手段22、送信側認証手段23、認証数カウント手段24、認証上限数格納手段25、カウント調整・判定手段26、デバイス情報格納手段27から構成される。

送信側D-I/F21は、著作権保護が必要なAVデータをアイソクロナスパケットとしてIEEE1394バス#1(1)に送信し、またIEEE1394バス#1(1)に接続されている他の機器とアシンクロナスパケットでコマンドなどを送受信するためのデジタルインターフェースである。

暗号化手段 22 は、チューナ（図示せず）から受信された AV データを暗号化する手段である。

送信側認証手段 23 は、シンク 0（4）、シンク 1（5）など、IEEE 1394 バス #1（1）に接続された機器と AV データを使用するための認証と、AV データの使用を中止するための認証であるデクレメント認証とを行う手段である。この AV データを使用するための認証（以下、単に認証と言う場合は、AV データを使用するための認証のことを意味するものとする）と、AV データの使用を中止するための認証であるデクレメント認証（以下、AV データの使用を中止するための認証のことをデクレメント認証と呼ぶ）は、異なった認証ルールによって行われる。

認証数カウント手段 24 は、送信側認証手段 23 が、認証を行い成功した数である認証数を、カウント調整・判定手段 26 の判定結果に応じて、数える手段である。

認証上限数格納手段 25 は、STB 20 が送信する著作権保護が必要な AV データを同時に受信して使用出来る機器の台数の上限を格納する手段である。

デバイス情報格納手段 27 は、送信側認証手段 23 が認証を行い成功した機器のデバイス ID を格納する手段である。ここで、デバイス ID とは、予め鍵管理センターから与えられているものであり、機器を特定するための情報である。

カウント調整・判定手段 26 は、デバイス情報格納手段 25 に格納されているデバイス ID を利用して、送信側認証手段 23 が認証を行い成功した場合、その認証が同一機器との重複した認証であるかどうか調べることによって、認証数カウント手段 24 が数えている認証数をカウントアップするかどうかを判定し、また送信側認証手段 23 が後述するデクレメント認証を行い成功した場合、認証数カウント手段 24 がカウントしている認証数をカウ

トダウンさせるかどうか判定する手段である。

送信側認証ルール格納手段 29 は、送信側認証手段 23 が行う認証とデクレメント認証とのそれぞれの認証ルールを格納する手段である。

送信側認証選択手段 28 は、送信側認証手段 23 が認証を行う際には、その認証ルールを選択し、デクレメント認証を行う際には、そのデクレメント認証用の認証ルールを選択するための手段である。

シンク 0 (4)、シンク 1 (5)、シンク 3 (9)、シンク 4 (8) はそれぞれ同様の構成を持つ。図 3 に TV 30 として、一台のシンクの構成を示す。

TV 30 は、受信側 D-I/F 31、復号手段 32、認証要求手段 33、受信側認証手段 34、受信側認証選択手段 35、受信側認証ルール格納手段 36 から構成される。

受信側認証選択手段 35 は、アイソクロナスパケットとして IEEE 1394 バス #2 (2) に送信された著作権保護が必要な AV データを受信し、また IEEE 1394 バス #1 (1) に接続されている他の機器とアシンクロナスパケットでコマンドなどを送受信するためのデジタルインターフェースである。

復号手段 32 は、受信した著作権保護が必要な AV データの暗号を復号する手段である。復号手段 32 で復号され平文になった AV データはデコーダ (図示せず) でデコードされ、モニタ (図示) に表示される。

認証要求手段 33 は、認証を行うよう要求するための認証コマンド (以下、認証コマンドと呼ぶ) とデクレメント認証を行うよう要求するデクレメント認証用の認証コマンド (以下、デクレメント認証用コマンドと呼ぶ) を STB 20 に送信する手段である。認証を行うための認証コマンドとデクレメント認証を行うためのデクレメント用認証コマンドは異なってコマンドが用いられる。

受信側認証手段 3 4 は、S T B 2 0 の送信側認証手段 2 3 と認証及びデクレメント認証を行う手段である。

受信側認証選択手段 3 5 は、受信側認証手段 3 4 が認証を行う際には認証のための認証ルールを選択し、受信側認証手段 3 4 がデクレメント認証を行う際には、デクレメント認証用の認証ルールを選択する手段である。

受信側認証ルール格納手段 3 6 は、認証のための認証ルールとデクレメント認証のための認証ルールを格納する手段である。

なお、本実施の形態の I E E E 1 3 9 4 バス # 1 (1) 、 I E E E 1 3 9 4 バス # 2 (2) は本発明のネットワークの例であり、本実施の形態のソース 3 すなわち S T B 2 0 は本発明の送信装置の例であり、本実施の形態のシンク 1 (5) すなわち T V 3 0 は本発明の受信装置の例であり、本実施の形態の送信側認証ルール格納手段 2 9 、送信側認証手段 2 8 、送信側認証手段は、本発明の送信側認証手段の例であり、本実施の形態の認証上限数格納手段 2 5 、認証数カウント手段 2 4 、カウント調整・判定手段 2 6 は本発明の認証数カウント手段の例であり、本実施の形態の受信側認証ルール格納手段 3 6 、受信側認証選択手段 3 5 、受信側認証手段 3 5 は本発明の受信側認証手段の例であり、本実施の形態のカウント調整・判定手段 2 6 は本発明の重複判定手段の例であり、本実施の形態のデバイス情報格納手段 2 7 は本発明の登録手段の例であり、本実施の形態の復号手段 3 2 で復号され平文になった A V データはデコーダ (図示せず) でデコードされ、モニタ (図示) に表示されるとは、本発明の著作権保護が必要なデータを使用することの例である。

次に、このような本実施の形態の動作を説明する。

まず、ソース 3 が I E E E 1 3 9 4 バス # 1 に送信した著作権保護が必要な A V データをシンク 1 (5) が受信して、シンク 1 (5) のモニタにその映像音声を表示するまでの動作を説明する。

著作権保護が必要なAVデータはMPEGトランスポートストリームであり、ソース3であるSTB20の図示していないチューナで受信されたものとする。そして、ソース3であるSTB20が送信する著作権保護が必要なAVデータは同時に最大3台までの機器しか受信して使用出来ないという制限が設けられているとする。

この制限を示す情報は、放送局でAVデータを送信する際にMPEGトランスポートストリームの内部に埋め込まれる。STB20は、チューナで受信したMPEGトランスポートストリームの内部からこの情報を取り出し、認証上限数格納手段25は、取り出された情報を参照することによって、認証上限数として3を設定する。

STB20がチューナで受信したAVデータをIEEE1394バス#1(1)に送信するためには、まず、送信側D-I/F21は、IEEE1394バス#1(1)のアイソクロナスリソースマネージャに使用する伝送帯域を指定してチャンネル使用权を要求する。そして、アイソクロナスリソースマネージャからチャンネル使用权が与えられたとする。

そうすると、暗号化手段22は、チューナで受信された著作権保護が必要なAVデータを暗号化して、送信側D-I/F21に出力する。

送信側D-I/F21は、暗号化されたAVデータからそのヘッダにアイソクロナスチャンネルの番号と自らのノードIDを付加したアイソクロナスパケットを作成し、作成したアイソクロナスパケットをIEEE1394バス#1(1)に送信する。

このようにしてSTB20は、著作権保護が必要なAVデータをIEEE1394バス#1(1)に送信する。

図4に機器が認証要求する毎に、認証数カウント手段24がカウントしている認証数とデバイス情報格納手段27が格納しているデバイスIDがどのように変化していくかを示す。現時点では、まだSTB20は認証要求を受

けておらず、認証数カウント手段24がカウントしている認証数は0であり、デバイス情報格納手段27には、いずれの機器のデバイスIDも格納していない。

一方、シンク1(5)がソース3が送信しているAVデータを受信して使用する場合には、まず、ソース3であるSTB20に認証要求を行う。

すなわち、シンク1(5)であるTV30の受信側D-I/F31は送信されてくるアイソクロナスパケットを受信して、そのヘッダ情報から送信元のノードIDを取得する。そして、認証要求手段30は、認証を要求するための認証コマンドを受信側D-I/F31に出力する。TV30には予め鍵管理センターからデバイスIDが割り当てられており、このデバイスIDによってTV30などの各機器を一意に特定することが出来る。そして、認証要求手段30が出力した認証コマンドには、TV30のデバイスIDが付加されている。

受信側D-I/F30は、認証コマンドを受け取ると、認証コマンドから先に取得した送信元のノードIDと自らのノードIDをヘッダに付加したアシンクロナスパケットを作成し、IEEE1394バス#(1)に送信する。

そして、受信側認証手段34は、受信側認証選択手段35に認証のための認証ルールを選択するよう指示し、これを受けて、受信側認証選択手段35は、受信側認証ルール格納手段36から認証のための認証コマンドを選択する。

受信側D-I/F31は、認証コマンドをアシンクロナスパケットとして、STB20に送信する。

STB20の送信側D-I/F21は、TV30の受信側D-I/F31からアシンクロナスパケットとして送られてきた認証コマンドを受信すると、認証コマンドを送信側認証手段23に出力する。

送信側認証手段23は、カウント調整・判定手段26にTV30のデバイ

スIDを通知し、判定を依頼する。

カウント調整・判定手段26は、送信側認証手段23からの依頼を受けて、受け取ったデバイスIDがすでにデバイス情報格納手段27に格納されているかどうかを判定する。そして、認証数カウント手段24がカウントしている認証数と認証上限数格納手段25に格納されている認証数の上限値を参照し、次のようにしてTV30からの認証要求を受理するか拒絶するかを判定する。

すなわち、この認証数が認証数の上限値より小さい場合、認証コマンドを受理すべきと判定する。また、この認証数が上限値と等しいかそれ以上の値であっても、受け取ったデバイスIDがデバイス情報格納手段27にすでに格納されている場合には、認証コマンドを受理すべきと判定する。そして、認証数が認証数の上限値と等しいかそれ以上の値であり、かつ受け取ったデバイスIDがデバイス情報格納手段27に格納されていない場合には、TV30からの認証コマンドを拒絶すべきと判定する。

送信側認証手段23は、この判定結果に従って、受信側認証手段34と認証を行うかどうかを決定する。

例えば、現時点では、認証上限数格納手段25が格納している上限数は3であり、認証数カウント手段24がカウントしている認証数が0であるので、認証数の上限より認証数が小さいので、カウント調整・判定手段26は認証要求を受理すべきと判定し、この判定結果に従って、送信側認証手段24は、受信側認証手段34と認証を行う。

すなわち、送信側認証手段23は、送信側認証選択手段28に認証ルールを選択するよう指示し、これを受けて、送信側認証選択手段28は、送信側認証ルール格納手段29から認証用の認証ルールを選択する。

送信側認証手段23は、送信側認証選択手段28が選択した認証のための認証ルールを用い、受信側認証手段34は、受信側認証選択手段34が選択

した認証のための認証ルールを用いて互いに認証を行う。

その結果TV30が正当な機器であり、認証が成功すると、送信側認証手段23と受信側認証手段34は、AVデータを暗号化及び復号するための鍵を交換する。従って、認証が成功すると、TV30は、STB20から送信されているAVデータの暗号を入手した鍵で復号して、デコードして、映像音声をモニタに表示して視聴することが出来る。

また、TV30が不正な機器であり、認証が失敗した場合には、上記の鍵の交換は行われない。従って、この場合にはTV30は、STB20が送信しているAVデータの暗号を復号することが出来ないので、AVデータをデコードしたとしても映像音声をモニタに表示して視聴することが出来ない。

このように著作権保護が必要なAVデータは暗号化されて伝送され、認証を行うことによって不正な機器を排除することが出来る。

このようにて認証が成功した場合、送信側認証手段23は、まず認証コマンドに付加されていたTV30のデバイスIDと認証が成功したことをカウント調整・判定手段26に通知する。

カウント調整・判定手段26は、認証が成功した通知を受け取ると、デバイス情報格納手段27が格納しているデバイス情報の中に通知されたTV30のデバイスIDがすでに格納されているかどうかを調べる。

そして、TV30のデバイスIDがデバイス情報格納手段27にまだ格納されていない場合には、新たにTV30のデバイスIDをデバイス情報格納手段27に格納する。

さらに、カウント調整・判定手段26は、TV30のデバイスIDがデバイス情報格納手段27に新規に格納した場合、認証数カウント手段24にカウントしている認証数を1だけカウントアップするよう指示する。TV30のデバイスIDがすでにデバイス情報格納手段27に格納されていた場合には、認証数カウント手段24にカウントしている認証数をカウントアップす

るよう指示しない。

認証数カウント手段 24 は、カウント調整・判定手段 26 からの指示に従って、カウントしている認証数を 1 だけカウントアップする。

従って、認証数カウント手段 24 は、同一機器と重複して行われた認証は数えない。

さらに、送信側認証手段 23 は、受信側認証手段 34 との認証で交換した鍵を暗号化手段 22 に渡す。

以後、暗号化手段 22 は、送信側認証手段 23 から渡された鍵で AV データを暗号化して送信側 D-I/F 21 に出力する。

一方、受信側認証手段 34 は、STB 20 との認証が成功した場合、その認証で交換した鍵を復号手段 32 に出力する。

これ以後、復号手段 32 は、STB 20 から送信されてきた AV データを、受信側認証手段 34 から受け取った鍵で復号し、復号され平文となった AV データは、図示していないデコーダでデコードされアナログ信号に変換されてモニタに表示される。

このようにて、シンク 1 (5) である TV 30 は、ソース 3 である STB 20 から送信される著作権保護が必要な AV データを受信してモニタに表示する。

つまり、図 4 に示すように、シンク 1 (5) が認証を要求して、STB 20 と認証を行った結果、成功すると、認証数カウント手段 24 がカウントしている認証数は 1 になり、デバイス情報格納手段 27 にはシンク 1 (5) のデバイス ID が格納される。

以上、ソース 3 が IEEE 1394 バス #1 に送信した著作権保護が必要な AV データをシンク 1 (5) が受信して、シンク 1 (5) のモニタにその映像音声を表示するまでの動作を説明した。

上記の動作と同様にして、ソース 3 が IEEE 1394 バス #1 (1) に

送信した著作権保護が必要なAVデータをシンク0(3)が受信してそのモニタに映像音声を表示出来たとする。すなわち、シンク0(4)とソース3とが認証した結果、その認証が成功したとする。

すなわち、シンク0(4)とソース3とが認証を行う際、シンク0(4)からの認証要求を、送信側認証手段23が受信すると、カウント調整・判定手段26に認証要求を受理すべきかどうかの判定を依頼する。

カウント調整・判定手段26は、認証数カウント手段24がカウントしている認証数が1であり、認証上限数格納手段25に格納されている上限数が3であり、認証数の方が上限数よりまだ小さいので、認証を受理するよう判定する。

そして、送信側認証手段23はこの判定に従ってシンク0(4)と認証を行う。

認証が成功すると、カウント調整・判定手段26は、デバイス情報格納手段27にすでにシンク0(4)のデバイスIDが格納されているかどうかを調べる。この時点で、デバイス情報格納手段27に格納されているデバイスIDはシンク1(5)のデバイスIDだけであるので、シンク0(4)のデバイスIDはまだ格納されていない。従って、認証数カウント手段24がカウントしている認証数を1カウントアップするよう指示する。

認証数カウント手段24は、カウント調整・判定手段26からの指示に従って、認証数を1だけカウントアップする。従って、認証数カウント手段24がカウントしている認証数は現時点で2となる。

以下、上記と同様にしてシンク0(4)は、ソース3から送信されてくるAVデータを復号して、モニタにその映像を表示することが出来るようになる。

すなわち、図4に示すように、シンク0(4)が認証要求を行い、STB20とシンク0(4)が認証を行い、成功すると、認証数カウント手段24

がカウントしている認証数は2にカウントアップされ、デバイス情報格納手段27には、シンク1(5)が追加されて、シンク1(5)とシンク0(4)のデバイスIDが格納されることになる。

ここで、シンク3(7)がソース3に認証要求を行い認証が成功したとすると、認証数カウント手段24がカウントしている認証数は3になり、デバイス情報格納手段27には、シンク0(4)、シンク1(5)、シンク3(7)のデバイスIDが格納されている。

すなわち、この時点でソース3が送信しているAVデータをモニタに表示している機器は3台である。

すなわち、図4に示すように、シンク3(7)が認証要求を行い、STB20とシンク3(7)が認証を行い、成功すると、認証数カウント手段24がカウントしている認証数は3にカウントアップされ、デバイス情報格納手段27には、シンク3(7)が追加されて、シンク1(5)とシンク0(4)とシンク3(7)のデバイスIDが格納されることになる。

ここで、4台目の機器としてシンク4(8)がソース3に認証要求したとする。カウント調整・判定手段26は、送信側認証手段23からシンク4(8)のデバイスIDと認証が要求されていることを通知されると、上記と同様にして、認証コマンドを受理するかどうかの判定を行う。この場合、デバイス情報格納手段27には、シンク0(4)、シンク1(5)、シンク3(7)のデバイスIDが登録されており、シンク4(8)のデバイスIDは登録されていない。そして、認証数カウント数手段24がカウントしている認証数は3であり、認証上限数格納手段25が格納している上限数は3である。

従って、デバイス情報格納手段27には、シンク4(8)のデバイスIDは登録されておらず、しかも認証数と上限数が等しくなっているので、カウント調整・判定手段26は、シンク4(8)からの認証コマンドを拒絶すべきと判定する。送信側認証手段23は、この判定に従って、シンク4(8)

からの認証要求を拒絶し、この認証は失敗する。

従って、シンク 4 (8) は、ソース 3 から送信されている AV データの暗号を復号することが出来ず、モニタにその映像音声を表示することが出来ない。

すなわち、図 4 に示すように、シンク 4 (8) が認証要求を行うと、STB 20 はその認証要求を拒絶し、認証数カウント手段 24 がカウントしているカウント数もデバイス情報格納手段 27 が格納しているデバイス ID も変化しない。

また、すでに認証に成功したシンク 0 (4) などの機器が重複して認証要求した場合、認証数カウント手段 24 がカウントしている認証数が上限数より小さくなくても、デバイス情報格納手段 27 にすでにシンク 0 (4) のデバイス ID が格納されているので、送信側認証手段 24 は認証を行う。そして、認証が成功しても、認証数カウント手段 24 は、カウントしている認証数をカウントアップしない。ただし、シンク 2 (ブリッジ装置) (6) などのブリッジ装置が再度認証要求を行った場合は、例外として認証数カウント手段 24 はカウントしている認証数をカウントアップする。そして、ブリッジ装置からの認証要求はブリッジ装置でない機器からの認証要求とは、別の形式を持つ。例えば、ブリッジ装置は、鍵管理センターからブリッジ装置でない機器とは異なった署名を与えられる。従って、ソース 3 は、認証コマンドに添付されている署名から認証要求を行った機器がブリッジ装置であるかどうかを判定することが出来る。

すなわち、図 4 に示すように、シンク 0 (4) が再度認証要求を行った場合、認証が行われ、その結果認証が成功した場合、認証数カウント手段 24 がカウントしている認証数 24 は 3 のままであり、またデバイス情報格納手段 27 が格納しているデバイス ID は、シンク 1 (5)、シンク 0 (4)、シンク 3 (7) のままである。

このように、ソース 3 は、認証数が上限数を越える場合に、まだ認証を行っていないシンクからの認証要求を拒絶する。従って、ソース 3 が送信している AV データを受信してモニタにその映像音声を表示出来るシンクの台数は最大でも 3 台に限定することが出来る。

次に、シンク 1 (5) が、ソース 3 から送信されてくる AV データをモニタに表示することを止める場合、シンク 1 (5) は、デクレメント認証を行うことによってソース 3 に通知する。以下、この場合の動作を説明する。

シンク 1 (5) である TV 30 の認証要求手段 33 は、AV データをモニタに表示することをやめることを通知するためにデクレメント認証用コマンドを受信側 D-I/F 31 に出力する。

このデクレメント用認証コマンドは、AV データをモニタに表示する際に予め行う認証のための認証コマンドとは、別に設けられている。すなわち、認証コマンドとデクレメント用認証コマンドとは、署名、演算式、認証方法が異なっている。

受信側 D-I/F 31 は、デクレメント用認証コマンドを上記で説明したのと同様にソース 3 である STB 20 に送信する。

送信側 D-I/F 21 は、デクレメント用認証コマンドを受信すると、送信側認証手段 23 に出力する。

そして、送信側認証手段 23 は、送信側認証選択手段 28 が選択した送信側デクレメント用認証ルールを使用し、また、受信側認証手段 34 は、受信側認証選択手段 35 が選択した受信側デクレメント用認証ルールを使用し、デクレメント認証を行う。

そして、デクレメント認証が成功すると、送信側認証手段 23 は、カウント調整・判定手段 26 にデクレメント認証が成功したことを通知する。

カウント調整判定手段 26 は、デバイス情報格納手段 27 に格納されているシンク 1 (5) のデバイス ID を削除する。そして、認証数カウント手段

23にカウントしている認証数を1だけカウントダウンするように指示する。これを受けて認証数カウント手段24は、カウントしている認証数を1だけカウントダウンする。

一方、TV30では、デクレメント認証が成功すると、受信側認証手段34は、復号手段32にデクレメント認証が成功したことを通知する。

復号手段32は、受信側認証手段34からの通知に従って、STB20から送信されてくるAVデータを復号している鍵を削除する。

デクレメント認証の結果、認証数カウント手段24がカウントしているカウント数は2になり、上限数である3より小さくなった。また、デバイス情報格納手段27には、シンク1(5)のデバイスIDが削除され、シンク0(4)とシンク(3)の2台のデバイスIDが格納されている。

すなわち、図4に示すように、シンク1(5)がデクレメント認証を要求し、デクレメント認証に成功した場合、認証数カウント手段24がカウントしている認証数は、1だけカウントダウンされて2になり、デバイス情報格納手段27が格納しているデバイスIDからシンク1(5)のデバイスIDが削除されて、シンク0(4)、シンク3(7)のデバイスIDのみが格納されることになる。

ただし、シンク2(ブリッジ装置)(6)が著作権保護が必要なデータの使用を中止する際にもデクレメント認証を行うが、この場合、第5の実施の形態で説明するように、シンク2(ブリッジ装置)(6)は、複数回ソース3とデクレメント認証を行い、IEEE1394バス#2(2)に接続されているシンク5(9)などの全ての機器が著作権保護が必要なデータをデコードして表示することを中止した場合、デバイス情報格納手段27に格納されているシンク2(ブリッジ装置)(6)のデバイスIDの登録が削除される。すなわち、シンク2(ブリッジ装置)(6)がソース3から著作権保護が必要なデータの使用を中止するとは、IEEE1394バス#2(2)に

接続されているシンク 5 (9) などの全ての機器がそのデータの使用を中止したことを意味する。

この時点でシンク 4 (8) などが認証要求を行えば、認証数カウント手段 24 がカウントしている認証数がある上限数より小さいので、正当な機器であれば認証が成功する。

すなわち、図 4 に示すように、シンク 4 (8) が認証要求すると、認証が行われ、成功する。そして、その結果認証数カウント手段 24 がカウントしている認証数は 3 になり、デバイス情報格納手段 27 は、シンク 0 (4)、シンク 3 (7)、シンク 4 (8) のデバイス ID が格納されることになる。

このように、すでに認証を行い成功した機器は、AV データの使用を中止する際に、デクレメント認証を要求し、STB 20 は、デクレメント認証用コマンドを受信すると、デクレメント認証を行い、成功すると、デバイス情報格納手段 27 は、デクレメント認証を要求した機器のデバイス ID を削除し、認証数カウント手段 24 は、カウントしている認証数を 1 だけカウントダウンするので、同時に AV データを使用出来る機器の台数の制限を守りながら、他の機器が新たに AV データを使用することも出来る。また、デクレメント用認証コマンドが認証コマンドとは別に設けられているので、不正な機器がデクレメント認証を悪用することを防止することが出来る。

また、IEEE 1394 バス #1 (1) から、いずれかの機器が取り外された場合や新たに機器が IEEE 1394 バス #1 に接続された場合には、バスリセットが行われる。このようにバスリセットが発生すると、認証数カウント手段 24 がカウントしている認証数は 0 に初期化され、また、デバイス情報格納手段 27 が格納しているデバイス ID はすべて削除される。そして、TV 30 の復号手段 32 は、使用していた AV データを復号するための鍵を捨ててしまう。このようにバスリセットが発生した場合には、初期状態からの動作を繰り返す。

なお、本実施の形態では、認証コマンドとデクレメント用認証コマンドとは、署名、演算式、認証方法が異なっているとして説明したがこれに限らない。認証コマンドとデクレメント用認証コマンドとは、少なくとも署名、演算式、認証方法のいずれか1つ以上が異なっていさえすればよい。

さらに、本実施の形態では、IEEE 1394バス#(1)に接続されている機器の台数が6台の場合について説明したが、これに限らず、3台、10台、63台など要するに、63台以下の任意の台数が接続されていても構わない。

さらに、本実施の形態では、ソース3は、ブリッジ装置以外のシンク1(5)などの機器と認証を行い成功した後、所定の原因によって認証がリセットされるまでの間に認証が成功したシンク1(5)などの機器と再度認証を行うが、たとえその認証に成功しても、認証数カウント手段24はカウントしている認証数をカウントアップせず、またソース3は、シンク2(ブリッジ装置6などと認証を行い成功した後、所定の原因によって認証がリセットされるまでの間に認証が成功したシンク2(ブリッジ装置)(6)と再度認証を行い、その認証が成功した場合、認証数カウント手段24はカウントしている認証数をカウントアップするとして説明したが、これに限らない。ソース3は、ブリッジ装置以外のシンク1(5)などの機器と認証を行い成功した後、所定の原因によって認証がリセットされるまでの間に認証が成功したシンク1(5)などの機器から再度認証要求されると、その認証要求を拒絶する。ただし、ソース3がシンク2(ブリッジ装置)(6)と認証を行い成功した後、所定の原因によって認証がリセットされるまでの間にシンク2(ブリッジ装置)(6)から再度認証要求された場合には、その認証要求を受付ける。そして、ソース3がシンク2(ブリッジ装置)(6)との再度の認証に成功した場合、認証数カウント手段24はカウントしている認証数をカウントアップしても構わない。

(第2の実施の形態)

次に、第2の実施の形態について説明する。

本実施の形態の著作権保護システムを第1の実施の形態と同様に図1に示す。

図5に、本実施の形態のソース3をSTB40として示す。第1の実施の形態のSTB20との相違点は、STB40が、カウント調整・判定手段26の代わりに判定手段41を備える点である。

判定手段41は、第1の実施の形態で説明したカウント調整・判定手段26とは異なり、認証要求が重複した認証かどうかの判定を行わない。

また、シンク0(4)、シンク1(5)などは、第1の実施の形態と異なり、任意に再認証要求を行わない。すなわち、シンク0(4)、シンク1(5)などIEEE1394バス#1(1)に接続されている機器は、ソース3が鍵の更新を行うか、またはIEEE1394バス#1(1)でバスリセットが発生するまでは、重複した認証要求を行わない。それ以外は第1の実施の形態と同様である。

なお、本実施の形態のソース3すなわちSTB40は本発明の送信装置の例であり、本実施の形態の認証上限数格納手段25、認証数カウント手段24、判定手段41は本発明の認証数カウント手段の例である。

次に、このような本実施の形態の動作を第1の実施の形態との相違点を中心に説明する。

第1の実施の形態と同様にソース3としてのSTB40の認証上限数格納手段25には3が格納されているとする。すなわち、STB40が送信する著作権保護が必要なAVデータは同時に最大3台までの機器によりモニタに表示して視聴することが出来る。

まだ、シンク1(5)などいずれの機器からも認証要求を受けていない場合、図6に示すように、ソース3としてのSTB40の認証数カウント手段

24がカウントしている認証数は0であり、デバイス情報格納手段27は、いずれの機器のデバイスIDも格納していない。

ここで、シンク1(5)が認証要求を行うと第1の実施の形態と同様にして、認証が行われ、成功する。その結果、図6に示すように、認証数カウント手段24がカウントしている認証数は1になり、デバイス情報格納手段27は、シンク1(5)のデバイスIDを格納する。

さらに、シンク0(4)が認証要求を行うと第1の実施の形態と同様にして、認証が行われ、成功する。その結果、図6に示すように、認証数カウント手段24がカウントしている認証数は2になり、デバイス情報格納手段27は、シンク1(5)とシンク0(4)のデバイスIDを格納する。

さらに、シンク3(7)が認証要求を行うと、第1の実施の形態と同様にして、認証が行われ、成功する。その結果、図6に示すように認証数は3、格納しているデバイスIDは、シンク1(5)、シンク0(4)、シンク3(7)になる。

さらに、シンク4(8)が認証要求を行うと、認証上限数格納手段25が格納している上限数と認証数カウント手段24がカウントしている認証数が等しいので、第1の実施の形態と同様にして、認証要求が拒絶される。その結果、図6に示すように認証数は3のままであり、格納しているデバイスIDは、シンク1(5)、シンク0(4)、シンク3(7)のまま変化しない。

次に、第1の実施の形態では、シンク0(4)が再び認証要求を行ったが、本実施の形態のシンク1(5)としてのTV30の認証要求手段33は、再認証要求を任意に行わない。すなわち、STB40が鍵の更新を行うか、またはIEEE1394バス#1(1)でバスリセットが発生することによって認証がリセットされるまでは、重複して認証要求を行わない。

従って、判定手段41は、認証要求された場合、その認証要求が同一の機器から行われたものかどうかの判定は行わない。

以下、シンク 1 (5) がデクレメント認証を要求し、その後シンク 4 (8) が認証要求するが、その動作は図 6 に示すように、第 1 の実施の形態と同様であるので説明を省略する。

ただし、シンク 2 (ブリッジ装置) (6) などのブリッジ装置は、STB 40 が鍵の更新を行うか、または IEEE 1394 バス # 1 (1) でバスリセットが行われることによって認証がリセットされるまでに、ソース 3 に再度認証要求することが出来る。そしてシンク 2 (ブリッジ装置) (6) から再度認証要求され、認証を行い成功した場合、認証数カウント手段 24 は、カウントしている認証数をカウントアップする。

ところで、STB 40 は、所定の時間が経過する毎に AV データを暗号化する鍵を別の鍵に更新する。このとき認証をリセットする。すなわち、今まで AV データを暗号化していた鍵の代わりに別の鍵で AV データを暗号化する。

また、STB 40 は、上記のように別の鍵に更新した場合、認証数カウント手段 24 がカウントしている認証数を 0 に初期化し、デバイス情報格納手段 27 に格納していたデバイス ID も削除する。

すなわち、STB 40 は、どの機器とも認証をしていない初期状態と同様の状態に戻る。

そして、STB 40 が鍵の更新を行うと、TV 30 の復号手段 32 は、AV データを今までの鍵で復号することが出来なくなってしまう。

そこで、TV 30 の認証要求手段 33 は、STB 40 が鍵の更新を行ったことを確認してから再度認証要求を行う。

さらに、STB 40 と TV 30 が認証を行い成功した場合、送信側認証手段 23 は、受信側認証手段 34 に今回の鍵の更新の次の回に行われる鍵の更新で有効になる鍵をも受信側認証手段 34 に渡す。

従って、STB 40 が鍵の更新を行った後に、認証要求を行っても、復号

手段 3 2 は、S T B 4 0 が鍵の交換を行った際に有効になる鍵をすでに入手済みであるので、A V データの復号を継続して行うことが出来る。

また、I E E E 1 3 9 4 バス # 1 (1) でバスリセットが発生した場合も、認証がリセットされる。つまり、認証数カウント手段 2 4 がカウントしている認証数を 0 に初期化し、デバイス情報格納手段 2 7 に格納していたデバイス I D も削除する。

すなわち、S T B 4 0 は、どの機器とも認証をしていない初期状態と同様の状態に戻る。この場合も、上記と同様にして T V 3 0 の認証要求手段 3 3 は、S T B 4 0 が鍵の更新を行ったことを確認してから再度認証要求を行う。

このように、シンク 1 (5) などの機器が任意に再認証要求を行わないようにすることによっても第 1 の実施の形態と同様に同時に著作権保護が必要な A V データをモニタに表示することが出来る機器の台数を制限することが出来る。

(第 3 の実施の形態)

次に、第 3 の実施の形態について説明する。

本実施の形態の著作権保護システムを第 1 の実施の形態と同様に図 1 に示す。

図 7 に本実施の形態のソース 3 を S T B 4 2 として示す。本実施の形態の S T B 4 2 は第 1 の実施の形態の S T B 2 0 とは異なりデクレメント認証を行わず、その代わりに、S T B 4 2 は、シンク 1 (5) などが A V データをデコードしてモニタに表示することを中止したかどうかを定期的に調査する。すなわち、本実施の形態の S T B 4 2 は、第 1 の実施の形態の S T B 2 0 とは異なり、調査手段 4 3 と対応表格納手段 5 0 を備えており、また、認証ルール格納手段 2 9 及び送信側認証選択手段 2 8 を備えていない。

調査手段 4 3 は、シンク 1 (5) などが A V データをデコードしてモニタに表示することを中止したかどうかを定期的に調査する手段である。

対応表格納手段50は、IEEE1394規格において機器を一意に特定する情報であるノードユニークIDと鍵管理センターから署名の一部として割り当てられた機器を一意に特定する情報であるデバイスIDとを対応つける対応表を格納する手段である。

また、図8に本実施の形態のシンク1(5)などをTV44として示す。

本実施の形態のTV44は、第1の実施の形態のTV30とは異なり、AVデータをデコードしてモニタに表示することを中止する場合、デクレメント認証を要求しない。すなわち、TV44は、受信側認証ルール格納手段36及び受信側認証選択手段35を備えていない。

それ以外は、第1の実施の形態と同様である。

なお、本実施の形態のソース3すなわち、STB42は本発明の送信装置の例であり、本実施の形態のシンク1(5)すなわちTV44は本発明の受信装置の例であり、調査手段43、本実施の形態のカウント調整判定・手段26、対応表格納手段50、デバイス情報格納手段27は本発明の調査手段の例である。

次にこのような本実施の形態の動作を第1の実施の形態との相違点を中心に説明する。

図4に示すように、第1の実施の形態と同様にして、シンク1(5)、シンク0(4)、シンク3(7)、シンク0(4)までがこの順に認証要求を行った結果、ソース3としての認証数カウント手段24がカウントしている認証数が3であり、デバイス情報格納手段27が、シンク1(5)、シンク0(4)、シンク3(7)のデバイスIDを格納しているとする。ただし、STB42は送信側認証選択手段29及び送信側認証ルール格納手段28を備えていないので、TV44と認証を行う際、認証ルールの選択は行わない。同様にTV44も、認証ルールの選択は行わない。

シンク1(5)としてTV44がソース3としてのSTB42から送信さ

れてくるAVデータの映像音声をモニタに表示しているものとする。

調査手段43は、定期的に、シンク0(4)、シンク1(5)などIEEE1394バス#1(1)に接続されている機器毎のプラグの状態を調べている。

ここで、プラグとは、IEEE1394バスを用いて、AV機器のデータを伝送したり、機器制御を行うための規格であるIEC61883で規格化されているものであり、IEEE1394バスに接続された機器間の論理的な接続を管理するための概念である。以下、簡単にプラグについて説明する。

プラグには入力プラグと出力プラグの2種類がある。すなわち、機器がIEEE1394バスからAVデータを入力する機能を持っている場合、その機器は、同時に入力出来るAVデータの数つまり同時に入力出来るアイソクロナスチャンネルチャンネルの数と同じ数の入力プラグを持っており、機器がAVデータをIEEE1394バスに出力する機能を持っている場合、その機器は、同時に出力出来るAVデータの数つまり同時に出力出来るアイソクロナスチャンネルの数と同じ出力プラグを持っている。

そして、各機器は、一つの入力プラグに対応して、入力プラグの状態を保持するための一つのiPCR(入力プラグコントロールレジスタ)を持っている。また、一つの出力プラグに対応して、出力プラグの状態を保持するための一つのoPCR(出力プラグコントロールレジスタ)を持っている。

IEEE1394バスに接続された機器どうしがAVデータの送受信を行う場合には、その機器同士がコネクションを張る必要がある。すなわち、送信側の機器のoPCRと出力側の機器のiPCRにコネクションの種類(ブロードキャストコネクションまたはポイントツーポイントコネクション)や、コネクションの数や使用するチャンネル番号などiPCRとoPCRに必要な情報を設定することによって、コネクションを張る。また、IEEE1394バスに接続された機器がAVデータを受信し、デコードして表示する

ことを中止する際には、上記のコネクションを切断する必要がある。この際、iPCRやoPCRに設定されているコネクションの数を減算したり、登録されているコネクションの種類を解除したりすることによって、コネクションを切断する。従って、iPCRに設定されている状態を調べることによって、AVデータを機器が受信してデコード表示しているか、AVデータをデコード表示することを中止しているかを知ることが出来る。以上プラグについて説明した。

さて、シンク1(5)が、ソース3から送信されてくるAVデータを受信して、デコード表示することを中止したとする。そうすると、そのAVデータに対応するiPCRのコネクションの設定が解除される。

調査手段43は、シンク1(5)のiPCRの状態を調べた結果、シンク1(5)がソース3とのコネクションを切断したことがわかったとする。

そうすると、調査手段43は、シンク1(5)のノードユニークIDを取得し、カウント調整・判定手段26にシンク1(5)のノードユニークIDとシンク1(5)がソース3としてのSTB42とのコネクションを切断したことを通知する。

カウント調整・判定手段26は、調査手段43から通知されると、受け取ったノードユニークIDから、対応表格納手段50に格納されている対応表を利用して、ノードユニークIDに対応するシンク1(5)のデバイスIDを調べる。

上述したように、図4に示すようにソース3としての認証数カウント手段24がカウントしている認証数が3であり、デバイス情報格納手段27が、シンク1(5)、シンク0(4)、シンク3(7)のデバイスIDを格納している。

従って、カウント調整・判定手段26は、シンク1(5)のデバイスIDがすでにデバイス情報格納手段27に格納されているので、デバイス情報格

納手段 2 7 からシンク 1 (5) のデバイス ID を削除し、また認証数カウント手段 2 4 がカウントしている認証数を 1 だけカウントダウンするよう指示する。これを受けて認証数カウント手段 2 4 は、カウントしている認証数を 1 だけカウントダウンする。

このように、第 1 の実施の形態とは異なり、ソース 3 から送信されている AV データを受信して、デコード表示することを中止した機器を、ソース 3 である STB 4 2 の調査手段 4 3 が調査することによって、デクレメント認証をしなくても第 1 の実施の形態と同等の効果を得ることが出来る。

なお、本実施の形態では、調査手段 4 3 は、シンク 1 (5) などのプラグの状態を調べることによって、シンク 1 (5) などが AV データを受信してデコード表示することを中止したかどうかを調べるとして説明したが、これに限らない。以下に説明するようにしても構わない。

すなわち、調査手段 4 3 は、各機器のプラグの状態を調べる前に、IEEE 1394 バス # 1 (1) に接続されている機器の台数を調べ、この機器の台数が減少した時のみ、どの機器が IEEE 1394 バス # 1 から取り外されたかを調べ、IEEE 1394 バス # 1 から取り外された機器のノードユニーク ID を取得し、カウント調整・判定手段 2 6 にその機器のノードユニーク ID と機器がとりはずされたことを通知する。そして、カウント調整・判定手段 2 6 は、通知されたノードユニーク ID に対応するデバイス ID を対応表から求める。そしてカウント調整・判定手段 3 6 は、デバイス情報格納手段 2 7 にその求めたデバイス ID が既に登録済みであるかどうか調べる。登録済みである場合は、STB 4 2 と認証済みの機器が取り外されたことになるので、カウント調整・判定手段 2 6 は、認証数カウント手段 2 4 がカウントしている認証数をカウントダウンするよう指示する。この指示を受けて認証数カウント手段 2 4 は、カウントしている認証数をカウントダウンする。さらに、カウント調整・判定手段 2 6 は、デバイス情報格納手段 2 7 に格納

されている取り外された機器のデバイスIDを削除する。

ただし、ここでIEEE1394バス#1から取り外されるとは、IEEE1394バス#1(1)に接続するコネクタをIEEE1394バス#1(1)から取り外したことではなく、TV44が受信側D-I/F31とは別の系統から送られてくるデータを受信し、モニタに表示するようになったことを意味する。

(第4の実施の形態)

次に、第4の実施の形態について説明する。

本実施の形態の著作権保護システムを第1の実施の形態と同様に図1に示す。

図9に、本実施の形態のソース3をSTB45として示す。本実施の形態のSTB45は第2の実施の形態のSTB40とは異なりデクレメント認証を行わず、その代わりに、シンク1(5)などがAVデータをデコードしてモニタに表示することを中止したかどうかを定期的に調査する。すなわち、本実施の形態のSTB42は、第2の実施の形態のSTB40とは異なり、調査手段43と対応表格納手段50を備えており、また、認証ルール格納手段29及び送信側認証選択手段28を備えていない。

調査手段43は、シンク1(5)などがAVデータをデコードしてモニタに表示することを中止したかどうかを定期的に調査する手段である。

対応表格納手段50は、IEEE1394規格において機器を一意に特定する情報であるノードユニークIDと鍵管理センターから割り当てられた機器を一意に特定する情報であるデバイスIDとを対応つける対応表を格納する手段である。

また、図8に本実施の形態のシンク1(5)などをTV44として示す。TV44は第3の実施の形態と同様である。

すなわち、本実施の形態のTV44は、第1の実施の形態のTV30とは

異なり、AVデータをデコードしてモニタに表示することを中止する場合、デクレメント認証を要求しない。

それ以外は、第2の実施の形態と同様である。

なお、本実施の形態のソース3すなわちSTB45は本発明の送信装置の例であり、本実施の形態の対応表格納手段50、判定手段41、調査手段43、デバイス情報格納手段27は本発明の調査手段の例である。

次にこのような本実施の形態の動作を第2の実施の形態との相違点を中心に説明する。

図6に示すように、第2の実施の形態と同様にして、シンク1(5)、シンク0(4)、シンク3(7)、シンク4(8)までがこの順に認証要求を行った結果、ソース3としての認証数カウント手段24がカウントしている認証数が3であり、デバイス情報格納手段27が、シンク1(5)、シンク0(4)、シンク3(7)のデバイスIDを格納しているとする。ただし、STB45は送信側認証選択手段29及び送信側認証ルール格納手段28を備えていないので、TV44と認証を行う際、認証ルールの選択は行わない。同様にTV44も、認証ルールの選択は行わない。

シンク1(5)としてTV44がソース3としてのSTB42から送信されてくるAVデータの映像音声をモニタに表示しているものとする。

調査手段43は、定期的に、シンク0(4)、シンク1(5)などIEEE1394バス#1(1)に接続されている機器毎のプラグの状態を調べている。

ここで、シンク1(5)が、ソース3から送信されてくるAVデータを受信して、デコード表示することを中止したとする。そうすると、そのAVデータに対応するiPCRのコネクションの設定が解除される。

調査手段43は、シンク1(5)のiPCRの状態を調べた結果、シンク1(5)がソース3とのコネクションを切断したことがわかったとする。

そうすると、調査手段43は、シンク1(5)のノードユニークIDを取得し、カウント調整・判定手段26にシンク1(5)のノードユニークIDとシンク1(5)がソース3としてのSTB42とのコネクションを切断したことを通知する。

これ以後の動作は第3の実施の形態と同様にして、従って、カウント調整・判定手段26は、シンク1(5)のデバイスIDがすでにデバイス情報格納手段27に格納されているので、デバイス情報格納手段27からシンク1(5)のデバイスIDを削除し、また認証数カウント手段24がカウントしている認証数を1だけカウントダウンするよう指示する。これを受けて認証数カウント手段24は、カウントしている認証数を1だけカウントダウンする。

このように、第2の実施の形態とは異なり、ソース3から送信されているAVデータを受信して、デコード表示することを中止した機器を、ソース3であるSTB42の調査手段43が調査することによって、デクレメント認証をしなくても第2の実施の形態と同等の効果を得ることが出来る。

(第5の実施の形態)

次に、第5の実施の形態について説明する。

図1に本実施の形態の著作権保護システムを示す。

図5に本実施の形態のソース3をSTB40として示す。本実施の形態のSTB40は、第2の実施の形態で説明したものと同一である。

図3に、本実施の形態のIEEE1394バス#1(1)に接続されたシンク1(5)やIEEE1394バス#2(2)に接続されたシンク5(9)などをTV30として示す。本実施の形態のTV30は、第2の実施の形態で説明したものと同一である。

図10に、シンク2(ブリッジ装置)、(4)をブリッジ装置46として示す。

ブリッジ装置 46 は、IEEE 1394 バス # 1 (1) から受信したアイソクロナスパケットとして送られてきた AV データをいったん復号してから、ブリッジ装置 46 が持つ鍵で暗号化してアイソクロナスパケットとして IEEE 1394 バス # 2 (2) に送信し、このとき IEEE 1394 バス # 1 (1) から受信したアイソクロナスパケットのヘッダに付加されている送信元のノード ID を自らのノード ID に書き換えて送信する装置である。

ブリッジ装置 46 は、受信側 D-I/F 31、復号手段 32、受信側認証手段 34、鍵カウント手段 47、認証要求手段 47、受信側認証ルール格納手段 36、受信側認証選択手段 35、送信側 D-I/F 21、暗号化手段 22、送信側認証手段 23、認証数カウント手段 48、判定手段 41、デバイス情報格納手段 27、送信側認証ルール格納手段 29、送信側認証選択手段 28 から構成される。

鍵カウント手段 47 は、AV データを IEEE 1394 バス # 1 (1) に送信するソース 3 などの機器と認証を行い成功した数である鍵カウント数を数える手段である。

認証数カウント手段 48 は、シンク 5 (9) などの IEEE 1394 バス # 2 (2) に接続されているシンク 5 (9) などの機器と認証を行い成功した数である認証数を数える手段である。

それ以外は、第 2 の実施の形態と同様であるので、説明を省略する。

なお、本実施の形態のブリッジ装置 46 は本発明のブリッジ装置の例であり、本実施の形態の受信側認証ルール格納手段 36、受信側認証選択手段 35、受信側認証手段 34 は本発明のブリッジ装置の受信側認証手段の例であり、本実施の形態の送信側認証ルール格納手段 29、送信側認証選択手段 28、送信側認証手段 23 は本発明のブリッジ装置の送信側認証手段の例であり、本実施の形態の認証数カウント手段 48 は本発明のブリッジ装置の認証数カウント手段の例であり、本実施の形態の認証数カウント手段 48 がカウ

ントしている認証数は本発明のブリッジ装置の認証数カウント手段がカウントしている認証数の例であり本実施の形態の鍵カウント数は本発明の許可の上限数の例である。

次に、このような本実施の形態の動作を説明する。

図11にブリッジ装置46の動作を示すステートマシン図を示す。以下、このステートマシン図を参照して説明する。

ブリッジ装置46は、IEEE1394バス#1(1)においては、ソース3が送信したAVデータを受信するシンクとして機能し、IEEE1394バス#2(2)においては、シンク5などにAVデータを送信するソースとして機能する。

ブリッジ装置46の電源が入れられたり、IEEE1394バス#1(1)とIEEE1394バス#2(2)にブリッジ装置46が接続されるなどしてIEEE1394バス#2(2)のバスリセットが発生した場合、またIEEE1394バス#1(1)に機器が接続または取り外されるなどしてIEEE1394バス#1(1)にバスリセットが発生した場合、ブリッジ装置46は未認証(S0)の状態にリセットされる。すなわち、ブリッジ装置の認証はリセットされる。未認証(S0)の状態では、ブリッジ装置46の鍵カウント手段47がカウントしている鍵カウント数は0に、ブリッジ装置46の認証数カウント手段48がカウントしている認証数は0にそれぞれ初期化される。

未認証(S0)の状態からソースとの認証(S1)への遷移では、認証の初期化が行われる。すなわち、ブリッジ装置33の認証要求手段33は、認証要求するためのコマンドである認証コマンドを作成し、受信側D-I/F31に出力する。受信側D-I/F31は、認証コマンドをIEEE1394バス#1(1)のソース3に送信する。

ソースとの認証(S1)の状態では、図5に示すソース3としてのSTB

67.

40は、第2の実施の形態と同様にして、ブリッジ装置46からの認証コマンドを受信すると、認証コマンドを受理するか拒絶するかを判定する。そして、STB40がブリッジ装置46からの認証コマンドを拒絶した場合、またはブリッジ装置46からの認証コマンドを受理したが認証に失敗した場合には、ソースとの認証(S1)の状態から未認証(S0)の状態に遷移する。

また、STB40がブリッジ装置46からの認証コマンドを受理し、STB40の送信側認証手段23と、ブリッジ装置46の受信側認証手段34が認証を行い成功した場合には、ソースとの認証(S1)の状態から認証済み(S2)の状態に遷移する。このとき、ブリッジ装置46の鍵カウント手段47は、カウントしている鍵カウント数を1だけカウントアップ、すなわち1にする。

また、ソース3としてのSTB40の判定手段41は、認証に成功したので、STB40の認証数カウント手段24がカウントしているカウント数を1だけカウントアップするよう指示し、これを受けて、STB40の認証数カウント手段24はカウントしている認証数を1だけカウントアップする。このようなSTB40の動作については第2の実施の形態で詳細に説明した。

認証済み(S2)の状態では、ブリッジ装置46はソース3などと認証が成功した状態にある。

認証済み(S2)の状態では、IEEE1394#2(2)に接続されたシンク5(9)などの機器から認証要求されると、ブリッジ装置46の判定手段41は、次のように判断する。すなわち、現在ブリッジ装置の認証数カウント手段48がカウントしている認証数が0であり、鍵カウント手段47がカウントしている鍵カウント数が1であり、認証数の方が鍵カウント数より値が小さくなっている。この場合、シンク5(9)からの認証コマンドに応じて、ブリッジ装置46の送信側認証手段23がシンク5(9)と認証を行うべきと判定する。ブリッジ装置46の送信側認証手段23は、この判

定に従って、シンク 5 (9) と認証を行う。すなわち、認証済み (S 2) の状態からシンクまたは別ブリッジ (受信側) との認証 (S 3) の状態に遷移する。ブリッジ装置 4 6 の送信側認証手段 2 3 とシンク 5 (9) との認証が成功すると、ブリッジ装置 4 6 の認証数カウント手段 4 8 はカウントしている認証数を 1 だけカウントアップし、デバイス情報格納手段 2 7 は、シンク 5 (9) のデバイス ID を格納する。従って、鍵カウント手段 4 7 がカウントしている鍵カウント数は 1 であり、認証数カウント手段 4 8 がカウントしている認証数は 1 になった。そして、認証済み (S 2) の状態に遷移する。

ここで、さらに、シンク 6 (10) がブリッジ装置 4 6 に認証コマンドを送信したとする。この場合、ブリッジ装置 4 6 の送信側認証手段 2 3 がシンク 6 (10) からの認証コマンドを受け取ると、ブリッジ装置 4 6 の判定手段 4 1 は送信側認証手段 2 3 からの依頼に基づいて、次のように判定する。すなわち、現在、鍵カウント手段 4 7 がカウントしている鍵カウント数が 1 であり、ブリッジ装置 4 6 の認証数カウント手段 4 8 がカウントしている認証数も 1 であり、鍵カウント数と認証数が等しくなっている。鍵カウント数と認証数が等しい場合、判定手段 4 1 は、シンク 6 (10) からの認証要求をリトライ終了させ、まず、ソース 3 と認証を行うべきと判定する。送信側認証手段 2 3 はこの判定に従って、シンク 6 (10) からの認証要求をいったん拒絶して終了させる。そして、ブリッジ装置 4 6 の認証要求手段 3 3 はソース 3 に認証コマンドを送信する。すなわち、認証済み (S 2) の状態からソースとの認証 (S 4) の状態に遷移する。

第 2 の実施の形態では、説明しなかったが、ブリッジ装置 4 6 は IEEE 1394 バス # 1 (1) のシンク 2 (6) として、他のシンク 5 (9) などとは異なり重複して認証要求をソース 3 に行う。そして、ソース 3 としての STB 40 は、ブリッジ装置 4 6 と認証を行い成功する度に、認証上限数格納手段 2 5 の上限数を越えない範囲で、STB 40 の認証数カウント手段 2

4はカウントしている認証数をカウントアップする。STB40の判定手段41が認証要求を受理するか拒絶するかの判定はブリッジ装置46とシンク1(5)などの場合で全く同様に行う。

ソース3とブリッジ装置46の送信側認証手段34とが第2の実施の形態と同様にして認証を行い成功すると、鍵カウント手段47は、カウントしている鍵カウントを1だけカウントアップする。すなわち、ソースとの認証(S4)の状態から認証済み(S2)の状態に遷移する。この時点で、鍵カウント数は2になっており、認証数は1になっている。

認証済み(S2)の状態、シンク6(10)から再び認証コマンドを受信すると、ブリッジ装置46の判定手段41は、鍵カウント数が認証数より大きいので、シンク6(10)と認証すべきと判定する。すなわち、認証済み(S2)の状態からシンクまたは別ブリッジ(受信側)との認証(S3)の状態に遷移する。そして、シンクまたは別ブリッジ(受信側)との認証(S3)の状態、ブリッジ装置46の送信側認証手段23がシンク6(10)と認証を行い成功すると、ブリッジ装置46の認証数カウント手段48は、カウントしている認証数を1だけカウントアップし、デバイス情報格納手段27は、シンク6(10)のデバイスIDを格納する。そして、シンクまたは別ブリッジ(受信側)との認証(S3)の状態から認証済み(S2)の状態に遷移する。この状態で鍵カウント数は2であり、認証数は2になっている。

このようにブリッジ装置46がIEEE1394バス#2に接続されている機器から認証要求された際、ブリッジ装置46は、鍵カウント数が認証数より大きい場合、認証済み(S2)の状態からシンクまたは別ブリッジ(受信側)との認証(S3)の状態に遷移し、鍵カウント数と認証数が等しい場合には、その機器からの認証要求をリトライ終了させ、ソース3にと認証を

行う。すなわち、認証済み（S 2）の状態からソースとの認証（S 4）の状態に遷移する。すなわち、ブリッジ装置 4 6 は、IEEE 1394 バス # 2（2）に接続された機器から認証要求された場合、鍵カウント数と認証数の値を比較し、鍵カウント数の方が認証数より大きい場合には、IEEE 1394 バス # 2（2）に接続された機器と認証を行い、鍵カウント数と認証数が等しい場合には、認証要求した機器と認証を行う前に、ソース 3 と認証を行う。

また、IEEE 1394 バス # 1 に接続されているソース 3 は、第 2 の実施の形態で説明したように、同時に最大 3 台までの機器にのみ AV データをデコード表示出来るように制限する機器である。このように、ブリッジ装置 4 6 は、IEEE 1394 バス # 2 に接続されたシンクから認証要求された場合、その機器と認証を行う前に IEEE 1394 バス # 1 に接続されたソースと認証を行い、その認証が成功してから、IEEE 1394 バス # 2 に接続されたシンクと認証を行うので、ブリッジ装置 4 6 が存在していてもソース 3 から送信された著作権保護が必要な AV データの台数の制限を守ることが出来る。

さて、シンク 5（9）がソース 3 から送信された著作権保護が必要な AV データを受信してデコードし、モニタに表示することを中止するシンク 5（9）は、第 1 の実施の形態で説明したのと同様にして、ブリッジ装置 4 6 にデクレメント認証用コマンドを送信することによってデクレメント認証を要求する。すなわち、認証済み（S 2）の状態からシンクまたは別ブリッジ（受信側）とのデクレメント認証（S 5）の状態に遷移する。この時点で、鍵カウント手段 4 7 の鍵カウント数は 2 であり、ブリッジ装置 4 6 の認証数カウント手段 4 8 がカウントしている認証数も 2 である。

シンクまたは別ブリッジ（受信側）とのデクレメント認証（S 5）の状態では、ブリッジ装置 4 6 は、シンク 5（9）とデクレメント認証を行う。そし

て、デクレメント認証に成功した場合、ブリッジ装置46の認証数カウント手段48がカウントしている認証数を1だけカウントダウンし、デバイス情報格納手段27は、格納しているシンク5(9)のデバイスIDを削除する。そして、シンクまたは別ブリッジ(受信側)とのデクレメント認証(S5)の状態からソースとのデクレメント認証(S6)の状態に遷移する。一方、デクレメント認証に失敗した場合にはシンクまたは別ブリッジ(受信側)とのデクレメント認証(S5)から認証済み(S2)の状態に遷移する。

ソースとのデクレメント認証(S6)の状態では、ブリッジ装置46はソース3とデクレメント認証を行い、成功すると、鍵カウント数を1だけカウントダウンし、ソースとのデクレメント認証(S6)の状態から認証済み(S2)の状態に遷移する。また、デクレメント認証が失敗すると、鍵カウント数をカウントダウンせずにソースとのデクレメント認証(S6)の状態から認証済み(S2)の状態に遷移する。この時点で、鍵カウント数は1になり、ブリッジ装置46の認証数も1になっている。

引き続き、認証済み(S2)の状態では、IEEE1394バス#2に接続されている他の機器から認証要求やデクレメント認証要求された場合、上記の動作を繰り返す。

このように、IEEE1394バス#2(2)に接続された機器がAVデータを受信してデコード表示することを中止する場合、第2の実施の形態と同様にしてそのことをブリッジ装置46に申告し、ブリッジ装置46がデクレメント認証を行うことによって、IEEE1394バス#1(1)とIEEE1394バス#2(2)がブリッジ装置と接続されていても、第2の実施の形態と同様にIEEE1394バス#1(1)とIEEE1394バス#2(2)に接続されている機器が、新たにAVデータを使用することが出来るようになる。

ところで、IEEE1394では、ソース3は、アイソクロナスリソース

マネージャから帯域とチャンネルを割り当てられたら即アイソクロナスパケットを送らなければならない。ソース3は、送るべきAVデータがない場合は空のアイソクロナスパケットをIEEE1394バス#1に送る。そして、ソース3が空のアイソクロナスパケットさえもIEEE1394バス#1に送らなかった場合、DTCF方式では、ソース3の認証がリセットされる。

従って、ブリッジ装置46(S2)が、認証済み(S2)の状態にあり、ソース3からのアイソクロナスパケットの送信が途切れた場合、認証済み(S2)の状態から遷移し、鍵カウンタを0に初期化し、またブリッジ装置46の認証数カウント手段48がカウントしている認証数を0に初期化し、認証済み(S2)の状態に戻る。すなわち、ソース3の認証がリセットされると、ブリッジ装置46も認証をリセットする。

また、ソース3からのアイソクロナスパケットの送信は継続しているが、ブリッジ装置46からのアイソクロナスパケットの送信が途切れた場合、認証済み(S2)の状態から遷移し、ブリッジ装置46の認証数カウント手段23がカウントしている認証数を0に初期化して、再び認証済み(S2)の状態に戻る。すなわち、ブリッジ装置46は認証をリセットする。

また、認証済み(S2)の状態にあり、IEEE1394バス#2(2)に接続されているシンク5(9)などの機器がIEEE1394バス#2(2)から消失したことをブリッジ装置46が発見した場合、認証済み(S2)の状態からソースとのデクレメント認証(S6)の状態に遷移する。

そして、ソースとのデクレメント認証(S6)の状態では、ブリッジ装置46は、ソース3とデクレメント認証を行う。成功した場合に鍵カウンタ数を1だけカウントダウンし、認証済み(S2)の状態に遷移する。失敗した場合は、鍵カウンタ数をカウントダウンせずに認証済み(S2)の状態に遷移する。

このように、ブリッジ装置46がIEEE1394バス#1(1)とIE

IEEE 1394バス#2を接続している場合であっても、第2の実施の形態で説明したのと同等の効果を得ることが出来る。

なお、本実施の形態では、ブリッジ装置46は、IEEE 1394バス#2(2)に接続されている機器から認証要求された場合、鍵カウント手段47がカウントしている鍵カウント数とブリッジ装置46の認証数カウント手段48がカウントしている認証数との大小関係に基づいて、その機器と認証するか、その機器と認証する前にソース3と認証を行うかを判定したが、これに限らない。鍵カウント手段47を設けず、IEEE 1394バス#2(2)に接続されているシンクから認証要求された場合、その認証を行う前にソース3と認証し、ソース3との認証が成功した場合のみ、そのシンクと認証を行っても構わない。このようにしても本実施の形態と同等の効果を得ることが出来る。

(第6の実施の形態)

次に、第6の実施の形態について説明する。

本実施の形態の著作権保護システムを第5の実施の形態と同様に図1に示す。

図5に本実施の形態のソース3を、STB40として示す。STB40は第2の実施の形態で説明したものと同一である。

また、図3に、本実施の形態のIEEE 1394バス#1(1)に接続されたシンク1(5)やIEEE 1394バス#2(2)に接続されたシンク5(9)などをTV30として示す。TV30は第2の実施の形態で説明したものと同一である。

また、図10に、シンク2(ブリッジ装置)(4)として、ブリッジ装置46を示す。

本実施の形態のブリッジ装置46は第5の実施の形態と同様の構成を持つ。

次に、このような本実施の形態の動作を第5の実施の形態との相違点を中

心に説明する。

第5の実施の形態では、ブリッジ装置46は図11のステートマシン図において、未認証(S0)の状態からソースとの認証(S1)の状態、認証済み(S2)へ遷移する際、ソース3と一回だけ認証を行い、成功した場合鍵カウント手段47がカウントしている鍵カウント数は1に設定された。

これに対して本実施の形態では、未認証(S0)の状態からソースとの認証(S1)の状態、認証済み(S2)へ遷移する際、ブリッジ装置46の認証要求手段33は、ソース3と認証したい回数を付加した認証コマンドをソース3に送信する。

そして、ブリッジ装置46の受信側認証手段34は、認証要求する際に指定した回数だけソース3と認証を行う。一方、ソース3はブリッジ装置46の受信側認証手段34と認証を行う際、第2の実施の形態と同様に認証上限数格納手段25に格納されている上限数と、STB40の認証数カウント手段24がカウントしている認証数に基づき、ブリッジ装置46からの認証を拒絶するか認証を行うかを判定して認証を行う。

ブリッジ装置46がこのように指定した回数だけまとめて認証を行い成功した回数分だけ、鍵カウント手段47は、鍵カウント数をカウントアップする。

従って、上記の認証が成功した場合、認証済み(S2)の状態に遷移した時点で、認証要求手段33が認証コマンドに付加したソース3と認証したい回数が1より大きい場合、鍵カウント数は1より大きい値になっており、またブリッジ装置48の認証数カウント手段48の認証数は、0になっている。

これ以外は、第5の実施の形態と同様である。すなわち、本実施の形態のブリッジ装置46は認証したい回数をソース3に通知し、その回数だけ予め認証するので、IEEE1394#2(2)に接続されたシンク5などの機器から認証要求されても、その認証要求を一旦拒絶し、ソース3と認証し成

功してから再度、その認証要求した機器と認証を行うといった２段階の処理を行う必要がない。予めソース３と認証した回数分までは、IEEE 1394バス#２（２）に接続されたシンク５などの機器からの認証要求を即座に受理して、その機器と認証を行うことが出来る。従って、第５の実施の形態と同等の効果に加え、さらに、ブリッジ装置４６の認証要求に対する応答時間が短くなるという効果も得ることが出来る。

（第７の実施の形態）

次に、第７の実施の形態について説明する。

本実施の形態の著作権保護システムを第５の実施の形態と同様に図１に示す。

図５に本実施の形態のソース３を、STB４０として示す。STB４０は第２の実施の形態で説明したものと同一である。

また、図３に、本実施の形態のIEEE 1394バス#１（１）に接続されたシンク１（５）やIEEE 1394バス#２（２）に接続されたシンク５（９）などをTV３０として示す。TV３０は第２の実施の形態で説明したものと同一である。

また、図１０に、シンク２（ブリッジ装置）（６）として、ブリッジ装置４６を示す。

本実施の形態のブリッジ装置４６は第５の実施の形態と同様の構成を持つ。

次に、このような本実施の形態の動作を第５の実施の形態との相違点を中心に説明する。

第５の実施の形態では、IEEE 1394バス#２に接続されている機器からデクレメント認証を要求された場合、認証済み（Ｓ２）の状態からシンクまたは別ブリッジ（受信側）とのデクレメント認証（Ｓ５）の状態に遷移し、さらにソースとのデクレメント認証（Ｓ６）の状態に遷移し、再び認証済み（Ｓ２）の状態に遷移した。

すなわち、ブリッジ装置46は、IEEE1394バス#2(2)に接続されている機器とデクレメント認証を行って成功した場合、ブリッジ装置46の認証数カウント手段48がカウントしている認証数を1だけカウントダウンし、引き続いて、ソース3とデクレメント認証を行って成功した場合、鍵カウント手段47がカウントしている鍵カウント数を1だけカウントダウンした。

これに対して本実施の形態では、IEEE1394バス#2からデクレメント認証を要求された場合、認証済み(S2)の状態からシンクまたは別ブリッジ(受信側)とのデクレメント認証(S5)に遷移する。すなわち、ブリッジ装置46は、IEEE1394バス#2に接続されている機器とデクレメント認証を行い、その結果成功した場合、ブリッジ装置46の認証数カウント手段48がカウントしている認証数を1だけカウントダウンする。

次に、ソースとのデクレメント認証(S6)には遷移せず、認証済み(S2)の状態に遷移する。すなわち、引き続き、ソース3とはデクレメント認証しない。従って、鍵カウント手段47がカウントしている鍵カウント数は変化しない。

上記のデクレメント認証が行われてから、新たにIEEE1394バス#2に接続されている機器から認証要求されない時間が所定の時間、例えば5分間経過すると、ブリッジ装置46はソースとのデクレメント認証を行う。

まだ、ソースとのデクレメント認証をブリッジ装置46が行っていない状態で、IEEE1394バス#2(2)に接続されているシンク7(11)などの機器から認証要求された場合、認証数が鍵カウント数より値が小さいので、ブリッジ装置46は、その認証要求した機器と認証を行う前に、ソース3と認証を行う必要がないので、ブリッジ装置46は、第5の実施の形態に比較してIEEE1394バス#2(2)からの認証要求に対して素早く応答することが出来る。

従って、第5の実施の形態と同等の効果に加え、さらに、ブリッジ装置46の認証要求に対する応答時間が短くなるという効果も得ることが出来る。

なお、本発明は、上述した本発明の著作権保護システムの全部または一部の手段（または、装置、素子、回路、部等）の機能をコンピュータにより実行させるためのプログラムであって、コンピュータと協働して動作するプログラムである。

本発明は、上述した本発明の著作権保護システムの全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラムを担持した媒体であり、コンピュータにより読み取り可能且つ、読み取られた前記プログラムが前記コンピュータと協働して前記機能を実行する媒体である。

なお、本発明の一部の手段（または、装置、素子、回路、部等）、本発明の一部のステップ（または、工程、動作、作用等）とは、それらの複数の手段またはステップの内の、幾つかの手段またはステップを意味し、あるいは、一つの手段またはステップの内の、一部の機能または一部の動作を意味するものである。

また、本発明の一部の装置（または、素子、回路、部等）とは、それらの複数の装置の内の、幾つかの装置を意味し、あるいは、一つの装置の内の、一部の手段（または、素子、回路、部等）を意味し、あるいは、一つの手段の内の、一部の機能を意味するものである。

また、本発明のプログラムを記録した、コンピュータに読みとり可能な記録媒体も本発明に含まれる。

また、本発明のプログラムの一利用形態は、コンピュータにより読み取り可能な記録媒体に記録され、コンピュータと協働して動作する態様であっても良い。

また、本発明のプログラムの一利用形態は、伝送媒体中を伝送し、コ

ンピュータにより読みとられ、コンピュータと協働して動作する態様であっても良い。

また、本発明のデータ構造としては、データベース、データフォーマット、データテーブル、データリスト、データの種類などを含む。

また、記録媒体としては、ROM等が含まれ、伝送媒体としては、インターネット等の伝送媒体、光・電波・音波等が含まれる。

また、上述した本発明のコンピュータは、CPU等の純然たるハードウェアに限らず、ファームウェアや、OS、更に周辺機器を含むものであっても良い。

なお、以上説明した様に、本発明の構成は、ソフトウェア的に実現しても良いし、ハードウェア的に実現しても良い。

産業上の利用可能性

以上説明したところから明らかなように、本発明は、ネットワークにブリッジ装置が接続されていても、著作権保護が必要な信号を受け取ることが出来る受信機器の数を制限したいという著作権者の要望を守ることが出来る著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラムを提供することが出来る。

また、本発明は、著作権保護が必要な信号をうけとることが出来る受信機器の数を受信機器の台数を指定して制限するという著作権者の要望を守ることが出来る著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラムを提供することが出来る。

請 求 の 範 囲

1. ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも1台以上の受信装置と、

前記受信装置に、前記ネットワークを利用して前記著作権保護が必要なデータを送信する送信装置とを備えた著作権保護システムであって、

前記送信装置は、前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記受信装置は、前記送信側認証手段と認証を行う受信側認証手段を有し、

前記認証数に制限を設けたことを特徴とする著作権保護システム。

2. 前記認証数カウント手段は、前記送信側認証手段が認証を行い成功すると、前記認証数を加算することを特徴とする請求項1記載の著作権保護システム。

3. 前記受信装置は、前記送信装置と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度認証要求しないことを特徴とする請求項2記載の著作権保護システム。

4. 前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置は、再度認証要求することが出来ることを特徴とする請求項3記載の著作権保護システム。

5. 前記送信装置は、前記受信装置と認証を行い成功した場合、所定の

原因によって前記認証がリセットされない限り、再度前記受信装置から認証要求があってもその認証要求を受け付けないことを特徴とする請求項 2 記載の著作権保護システム。

6. 前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置は、前記ブリッジ装置から認証要求が行われた場合、その認証要求を受け付けることを特徴とする請求項 5 記載の著作権保護システム。

7. 前記送信装置は、前記受信装置と認証を行い成功した場合、再度前記受信装置と認証を行うが、所定の原因によって前記認証がリセットされない限り、たとえその認証に成功しても前記認証数カウント手段は、前記認証数を加算しないことを特徴とする請求項 2 記載の著作権保護システム。

8. 前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記認証数カウント手段は、再度前記ブリッジ装置と認証を行い成功した場合、前記認証数を加算することを特徴とする請求項 7 記載の著作権保護システム。

9. 前記送信側認証手段は、前記受信装置と認証を行い成功した場合、前記受信装置を特定する情報を登録する登録手段と、

前記受信装置から認証要求が行われると、その認証要求がすでに認証を行い成功した前記受信装置からの認証要求かどうかを登録した前記受信装置を特定する情報を利用して行う重複判定手段とを有することを特徴とする請求項 3～8 のいずれかに記載の著作権保護システム。

10. 前記認証のリセットは、鍵の更新が行われた時に起こることを特徴とする請求項3～8のいずれかに記載の著作権保護システム。

11. 前記認証のリセットは、交換鍵の更新が行われた時に起こることを特徴とする請求項3～8のいずれかに記載の著作権保護システム。

12. 前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置が前記鍵の更新を行った場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする請求項10記載の著作権保護システム。

13. 前記認証のリセットは、バスリセットされた際に起こることを特徴とする請求項3～8のいずれかに記載の著作権保護システム。

14. 前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置が接続されている前記ネットワークで、前記バスリセットされた場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする請求項13記載の著作権保護システム。

15. 前記認証数に制限を設けるとは、前記認証数が所定の値以上になった場合、前記送信側認証手段は、前記受信装置からの認証要求を受け付けないことであることを特徴とする請求項1記載の著作権保護システム。

16. 前記送信側認証手段と認証を行い成功した前記受信装置が、前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止した場合、前記認証数カウント手段は、前記認証数を減算することを特徴とする請

求項 1 記載の記載の著作権保護システム。

17. 前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止するとは、前記他のネットワークに接続されているすべての前記受信装置が前記送信装置から送られてくる前記著作権の保護が必要なデータの使用を中止したことであることを特徴とする請求項 16 記載の著作権保護システム。

18. 前記送信装置は、前記送信側認証手段と認証を行い成功した前記受信装置を特定する情報を登録する登録手段を有し、

前記認証数カウント手段が前記認証数を減算した場合、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録を解除することを特徴とする請求項 16 記載の著作権保護システム。

19. 前記送信装置は、前記受信装置が、前記著作権保護が必要なデータの使用を中止したかどうかを調査する調査手段を有することを特徴とする請求項 16 記載の著作権保護システム。

20. 前記著作権保護が必要なデータの使用を中止するとは、前記受信装置が前記ネットワークから切り離されることであり、

前記調査手段は、前記受信装置が前記ネットワークから切り離されたかどうかを定期的に調査することを特徴とする請求項 19 記載の著作権保護システム。

21. 前記調査するとは、前記ネットワークに接続されている前記受信装置の数である接続数を定期的に調査し、前記接続数が減少した場合、どの前記受信装置が前記ネットワークから切り離されたかをチェックすることであ

ることを特徴とする請求項 20 記載の著作権保護システム。

22. 前記調査手段は、前記受信装置の動作状態及び／または接続プラグのアクティブ状態を調べることによって、前記受信装置が前記著作権保護が必要なデータの使用中を中止したかをチェックし、

前記認証数カウント手段は、前記調査手段の調査の結果、前記受信装置が前記著作権保護が必要なデータを使用していないようであれば、前記認証数を減算することを特徴とする請求項 19 記載の著作権保護システム。

23. 前記調査手段は、前記受信装置を特定する情報と、その受信装置の署名とを対応付ける対応表を有し、

前記調査手段は、前記対応表を利用して、前記ネットワークから切り離された前記受信装置が認証済みであったかどうかを判定し、

前記認証数カウント手段は、前記判定結果が、前記ネットワークから切り離された前記受信装置が認証済みであったことを示す場合、前記認証数を減算することを特徴とする請求項 20 または 21 に記載の著作権保護システム。

24. 前記受信側認証手段は、前記受信装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用中を中止する場合、前記送信装置に前記認証数を減算するためのデクレメント認証要求を行い、

前記送信側認証手段は、前記受信側認証手段と、前記デクレメント認証を行い、

前記認証数カウント手段は、前記デクレメント認証が成功すると、前記認証数を減算することを特報とする請求項 16 記載の著作権保護システム。

25. 前記デクレメント認証を行うためのコマンドであるデクレメント認証用コマンドが、前記著作権保護が必要なデータを使用する際の認証を行うためのコマンドである認証コマンドとは別に作成されていることを特徴とする請求項 24 記載の著作権保護システム。

26. 前記著作権保護が必要なデータは暗号化されており、

前記デクレメント認証が成功すると、前記受信装置は、前記著作権保護が必要なデータを解読するための鍵を放棄することを特徴とする請求項24または25に記載の著作権保護システム。

27. 前記デクレメント認証は、前記著作権保護が必要なデータを使用するための認証とは、署名、認証方法、演算式の少なくとも1つ以上が異なっていることを特徴とする請求項24または25に記載の著作権保護システム。

28. 所定の原因によって認証がリセットされた場合、前記認証数カウント手段は、前記認証数を初期化し、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録をすべて解除することを特徴とする請求項18に記載の著作権保護システム。

29. 前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられていることを特徴とする請求項2に記載の著作権保護システム。

30. 前記ブリッジ装置は、前記他のネットワークでは、前記送信装置として扱われ、

前記他のネットワークに接続された前記受信装置から認証要求が行われた場合、

その受信装置と認証を行う前に、前記ネットワークに接続された前記送信装置と認証を行い、その送信装置との認証が成功した場合、前記受信装置と認証を行うことを特徴とする請求項29に記載の著作権保護システム。

31. 前記ブリッジ装置の前記認証数カウント手段が減算された場合、前記ブリッジ装置は、前記ネットワークに接続された前記送信装置と、前記ネットワークに接続された前記送信装置の前記認証数カウント手段がカウントしている前記認証数を減算させるためのデクレメント認証を行うことを特徴とする請求項29に記載の著作権保護システム。

32. 前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置

の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である認証数をカウントすることを特徴とする請求項 29 記載の著作権保護システム。

33. 前記ネットワークに新たに前記送信装置が接続された場合、前記ブリッジ装置は、前記ブリッジ装置の前記認証数カウント手段がカウントしていた前記認証数の回数だけ新たに接続された前記送信装置と認証を行うことを特徴とする請求項 32 記載の著作権保護システム。

34. 前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を有し、

前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である前記認証数をカウントし、

前記ブリッジ装置は、前記ネットワークに接続された前記送信装置と認証して成功した数を前記鍵カウンタがカウントしている前記許可の限度数とし、

前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数を減算するためのデクレメント認証要求があった場合、前記ブリッジ装置は前記ネットワークに接続されている前記送信装置とデクレメント認証を行わず、その受信装置とデクレメント認証を行い、

前記デクレメント認証が成功すると、前記ブリッジ装置の前記認証数カウント手段は、前記認証数を減算し、

前記他のネットワークに接続されている前記受信装置から新たに認証要求があった際、

前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウ

トしている前記認証数より小さい場合には、その受信装置と認証を行い、

前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より小さくない場合には、その受信装置と認証を行う前に前記ネットワークに接続されている前記送信装置と認証を行い、その認証が成功した場合、その受信装置と認証を行うことを特徴とする請求項 30 記載の著作権保護システム。

35. 前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から送られてくるデータを再暗号化して、前記他のネットワークに接続されている前記受信装置に送信し、

前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である認証数をカウントし、

前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を有することを特徴とする請求項 29 記載の著作権保護システム。

36. 前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数と前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きい場合、その認証要求を許可することを特徴とする請求項 35 記載の著作権保護システム。

37. 前記鍵カウント手段がカウントしている許可の限度数の上限は予め前記ネットワークに接続されている前記送信装置から与えられていることを特徴とする請求項 36 記載の著作権保護システム。

38. 前記鍵カウント手段がカウントしている許可の限度数の上限は、前記ブリッジ装置が前記ネットワークに接続されている前記送信装置と認証を

行うことによって、加算されることを特徴とする請求項 3 6 記載の著作権保護システム。

39. 前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、その認証要求を拒絶することを特徴とする請求項 3 5 記載の著作権保護システム。

40. 前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ネットワークに接続されている前記送信装置に前記許可の限度数を加算するよう依頼することを特徴とする請求項 3 5 記載の著作権保護システム。

41. 前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ネットワークに接続されている前記送信装置に認証要求を行い、前記認証が成功した場合、前記鍵カウント手段は、前記許可の限度数を加算することを特徴とする請求項 3 5 記載の著作権保護システム。

42. 前記ブリッジ装置は、前記他のネットワークに接続された前記受信装置から認証要求される毎に、前記ネットワークに接続された前記送信装置に前記他のネットワークに接続された前記受信装置のうち認証要求を行っているものの台数を通知することを特徴とする請求項 2 9 記載の著作権保護システム。

43. 前記ブリッジ装置が前記ネットワークに接続された前記送信装置に

対して認証要求を行うための認証コマンドには、前記台数を通知するためのフィールドが設けられており、前記ブリッジ装置は、前記フィールドを利用して前記台数の通知を行うことを特徴とする請求項 4 2 記載の著作権保護システム。

4 4. 前記ブリッジ装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドは、前記ブリッジ装置の機能を有しない前記ネットワークに接続された前記受信装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドとは区別されていることを特徴とする請求項 2 9 記載の著作権保護システム。

4 5. 前記区別は、前記認証コマンドに添付する署名によって行われることを特徴とする請求項 4 4 記載の著作権保護システム。

4 6. 送信装置と認証する受信側認証手段を有し、ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも 1 台以上の受信装置に対して、前記ネットワークを利用して前記著作権保護が必要なデータを送信する送信装置であって、

前記受信側認証手段と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記認証数に制限を設けたことを特徴とする送信装置。

4 7. ネットワークに接続され、著作権保護が必要なデータを受信して使用する受信装置であって、

前記受信装置と認証を行う送信側認証手段と、前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有する送信装置の前記送信側認証手段と認証する受信側認証手段を備え、

前記認証数に制限を設けたことを特徴とする受信装置。

4 8. 前記一方のネットワークに接続された送信装置から送信された著作

権保護が必要なデータを前記他のネットワークに接続された受信装置に送信するブリッジ装置であって、

前記受信装置と認証を行うブリッジ装置用送信側認証手段と、

前記送信側認証手段が認証した数であるブリッジ装置用認証数を数えるブリッジ装置用認証数カウント手段と、

前記送信装置と認証を行うブリッジ装置用受信側認証手段とを備え、

前記送信装置は、前記ブリッジ装置または前記ネットワークに接続された前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記受信装置は、前記ブリッジ装置または前記他のネットワークに接続された前記送信装置と認証する受信側認証手段を有し、

前記送信側認証手段が数える前記認証数に制限を設けたことを特徴とするブリッジ装置。

49. ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも一台以上の受信装置に、前記ネットワークを利用して送信装置から前記著作権保護が必要なデータを送信する著作権保護方法であって、

前記送信装置は、前記受信装置と認証した数である認証数を数え、

前記認証数に制限を設けたことを特徴とする著作権保護方法。

50. 請求項1記載の著作権保護システムの、前記受信装置における、前記送信側認証手段と認証を行う受信側認証手段と、

前記送信装置における、前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段との全部または一部としてコンピュータを機能させるためのプログラムを担持した媒体であって、コンピュータにより処理可能である媒体。

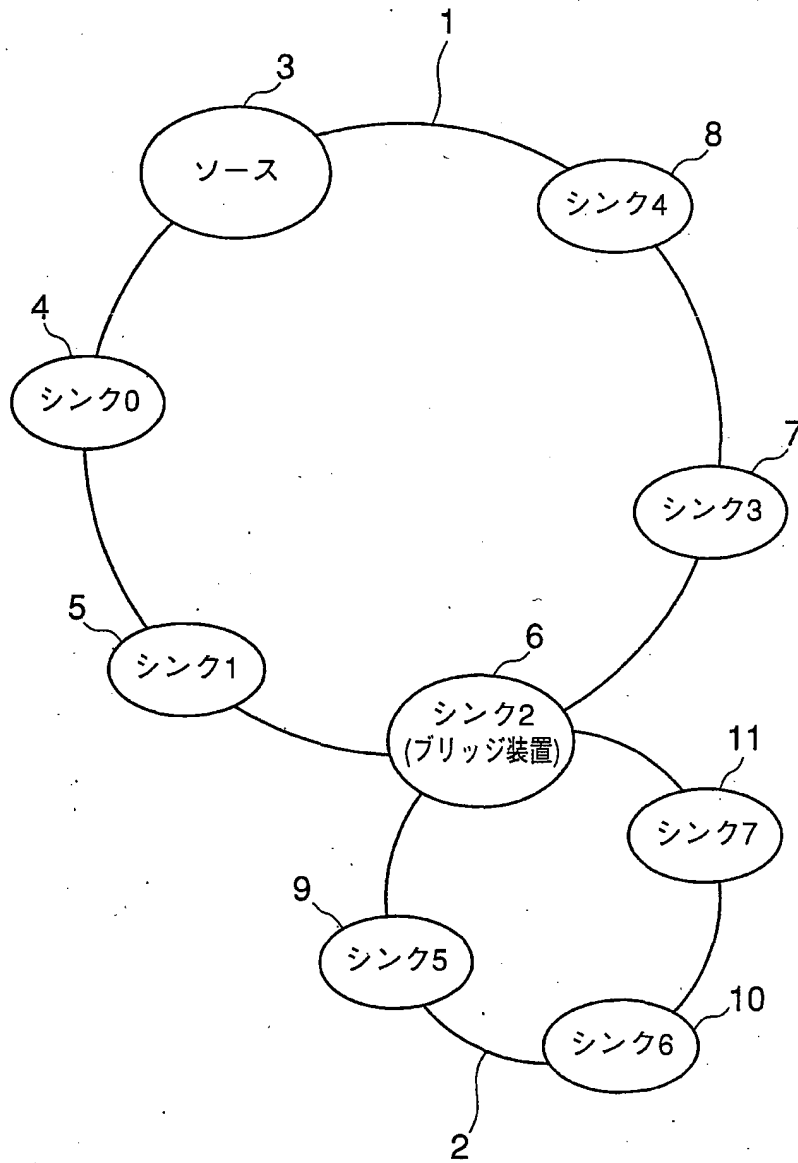
51. 請求項1記載の著作権保護システムの、前記受信装置における、前記送信側認証手段と認証を行う受信側認証手段と、

前記送信装置における、前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段との全部または一部としてコンピュータを機能させるためのプログラム。

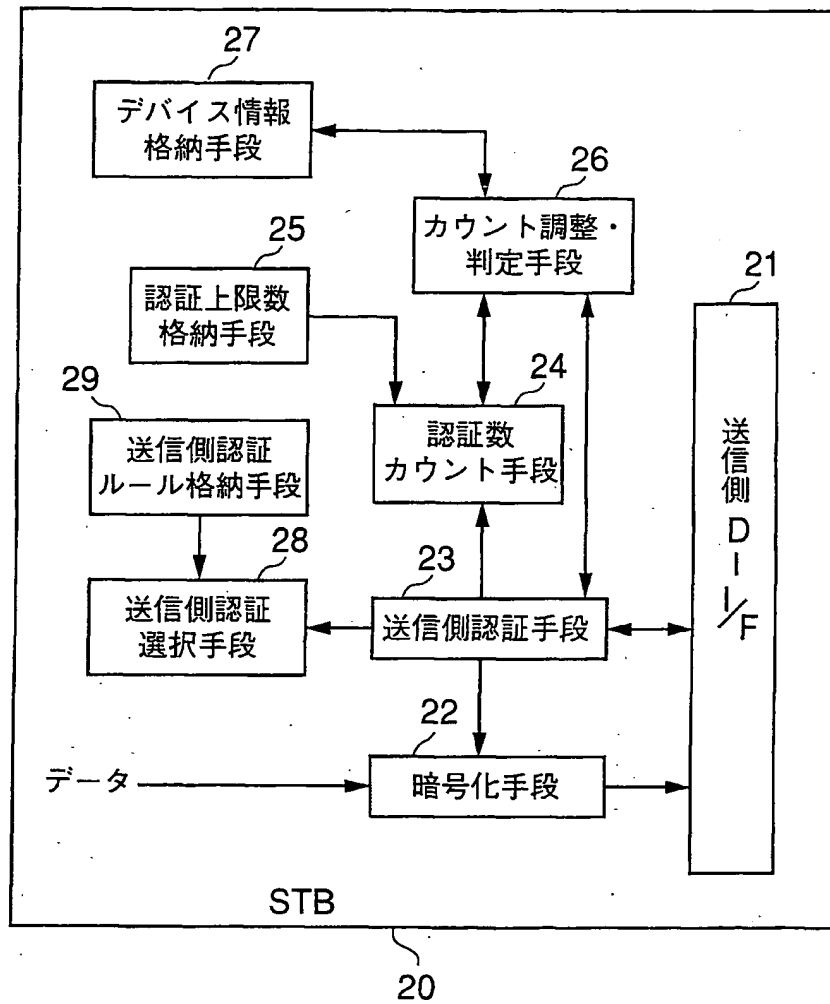
1 / 1 2

第 1 図



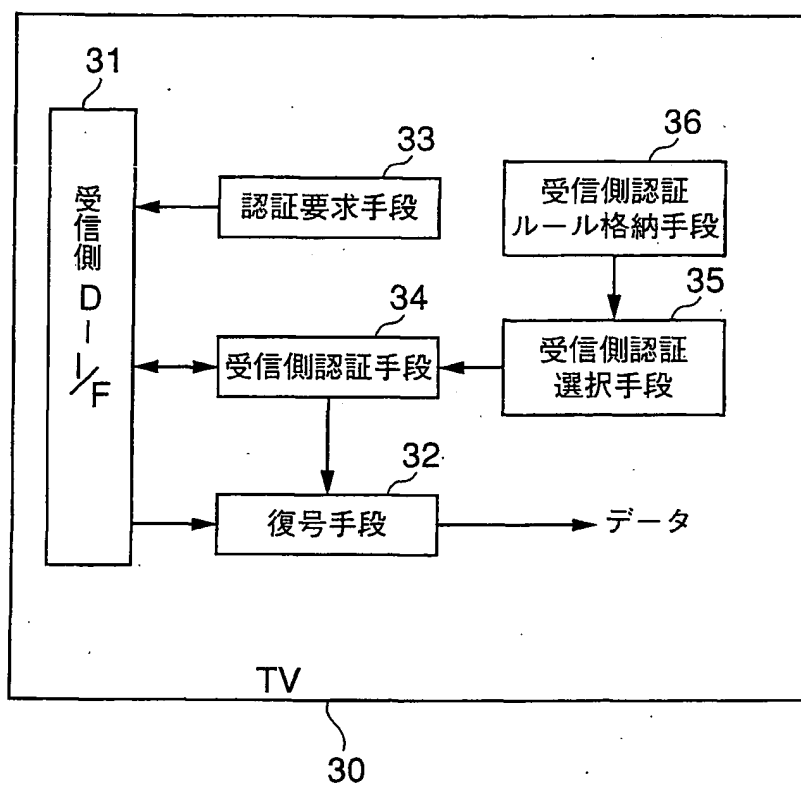
2 / 1 2

第 2 図



3 / 1 2

第 3 図



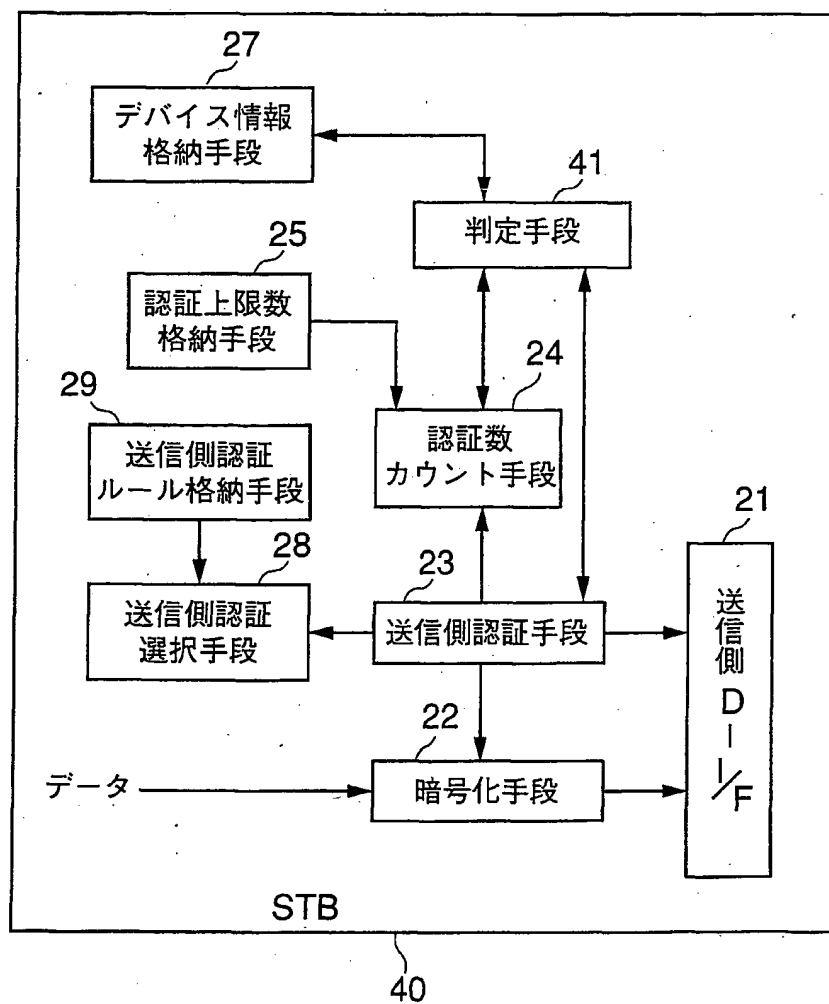
4 / 1 2

第 4 図

認証要求した機器	認証の種類	認証の結果	カウント している 認証数	格納しているデバイスID
なし	—	—	0	なし
シンク1(5)	認証	成功	1	シンク1(5)
シンク0(4)	認証	成功	2	シンク1(5), シンク0(4)
シンク3(7)	認証	成功	3	シンク1(5), シンク0(4), シンク3(7)
シンク4(8)	認証	拒絶	3	シンク1(5), シンク0(4), シンク3(7)
シンク0(4)	認証	成功	3	シンク1(5), シンク0(4), シンク3(7)
シンク1(5)	デクレメント 認証	成功	2	シンク0(4), シンク3(7)
シンク4(8)	認証	成功	3	シンク0(4), シンク3(7), シンク4(8)

5 / 1 2

第 5 図



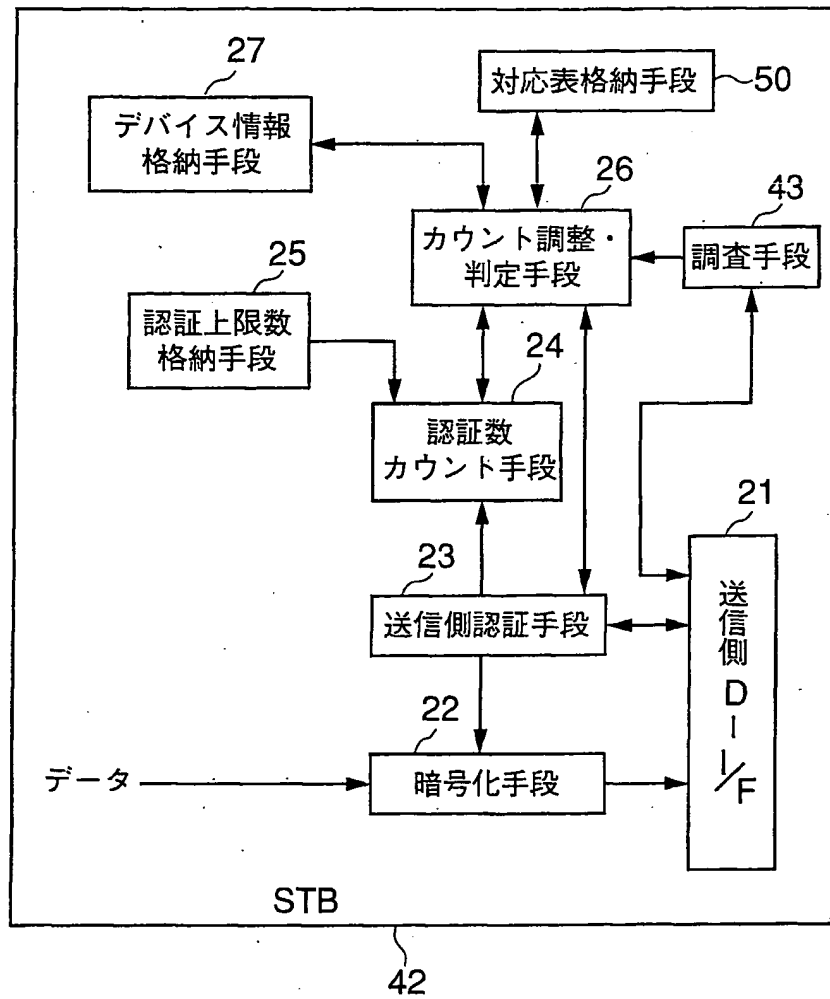
6 / 1 2

第 6 図

認証要求した機器	認証の種類	認証の結果	カウント している 認証数	格納しているデバイスID
			0	なし
シンク1(5)	認証	成功	1	シンク1(5)
シンク0(4)	認証	成功	2	シンク1(5), シンク0(4)
シンク3(7)	認証	成功	3	シンク1(5), シンク0(4), シンク3(7)
シンク4(8)	認証	拒絶	3	シンク1(5), シンク0(4), シンク3(7)
シンク1(5)	デクレメント 認証	成功	2	シンク0(4), シンク3(7)
シンク4(8)	認証	成功	3	シンク0(4), シンク3(7), シンク4(8)

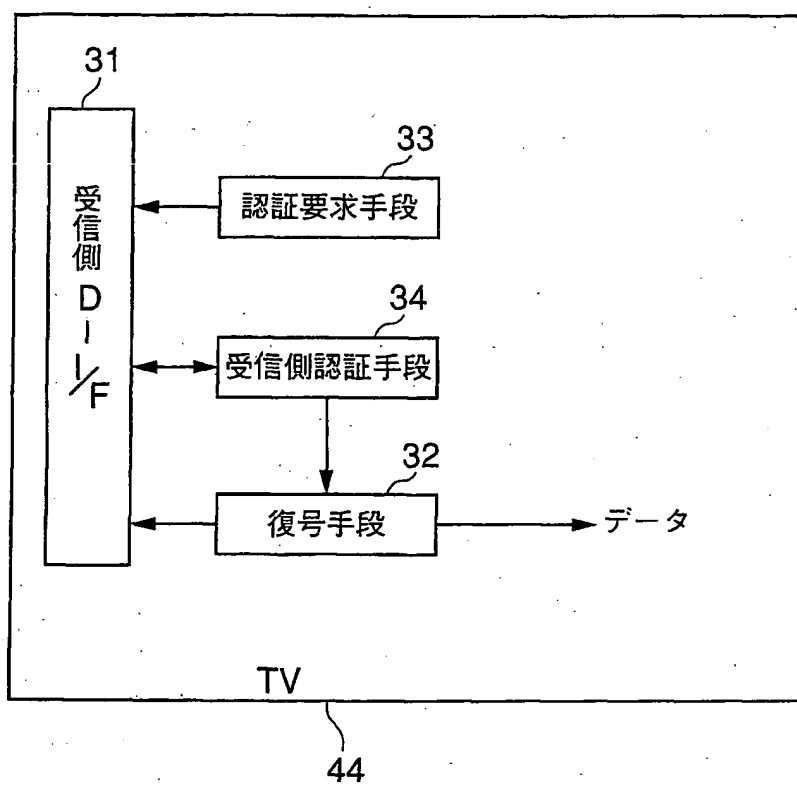
7/12

第7図



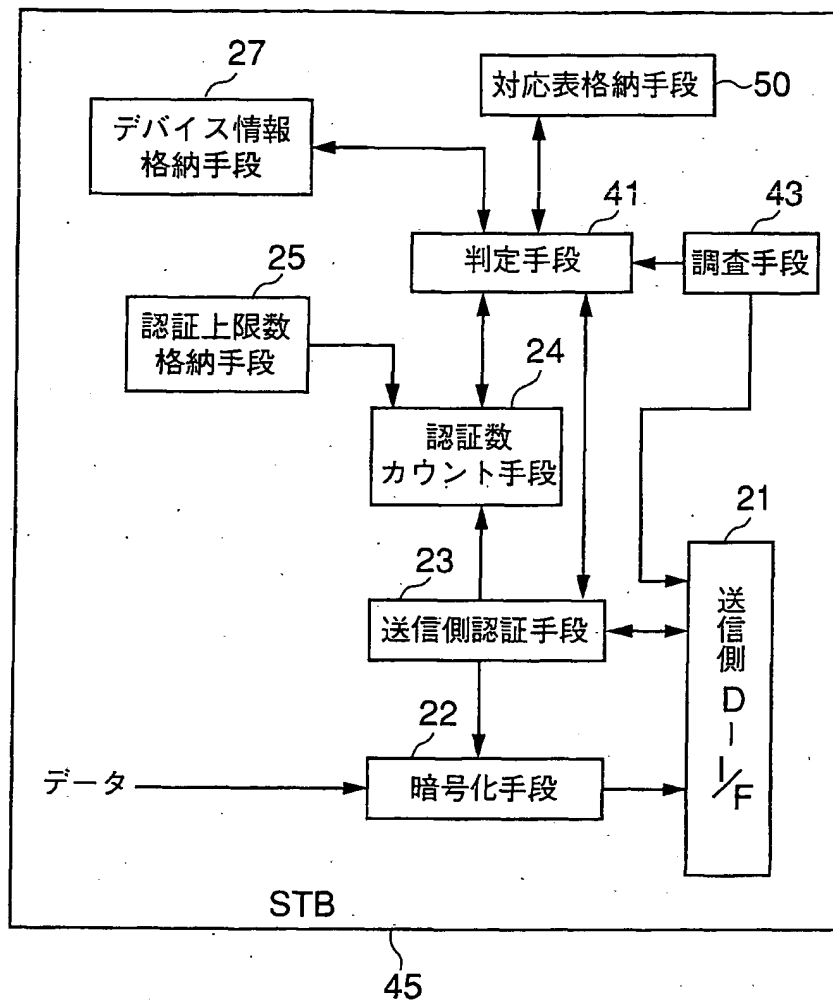
8 / 1 2

第 8 図



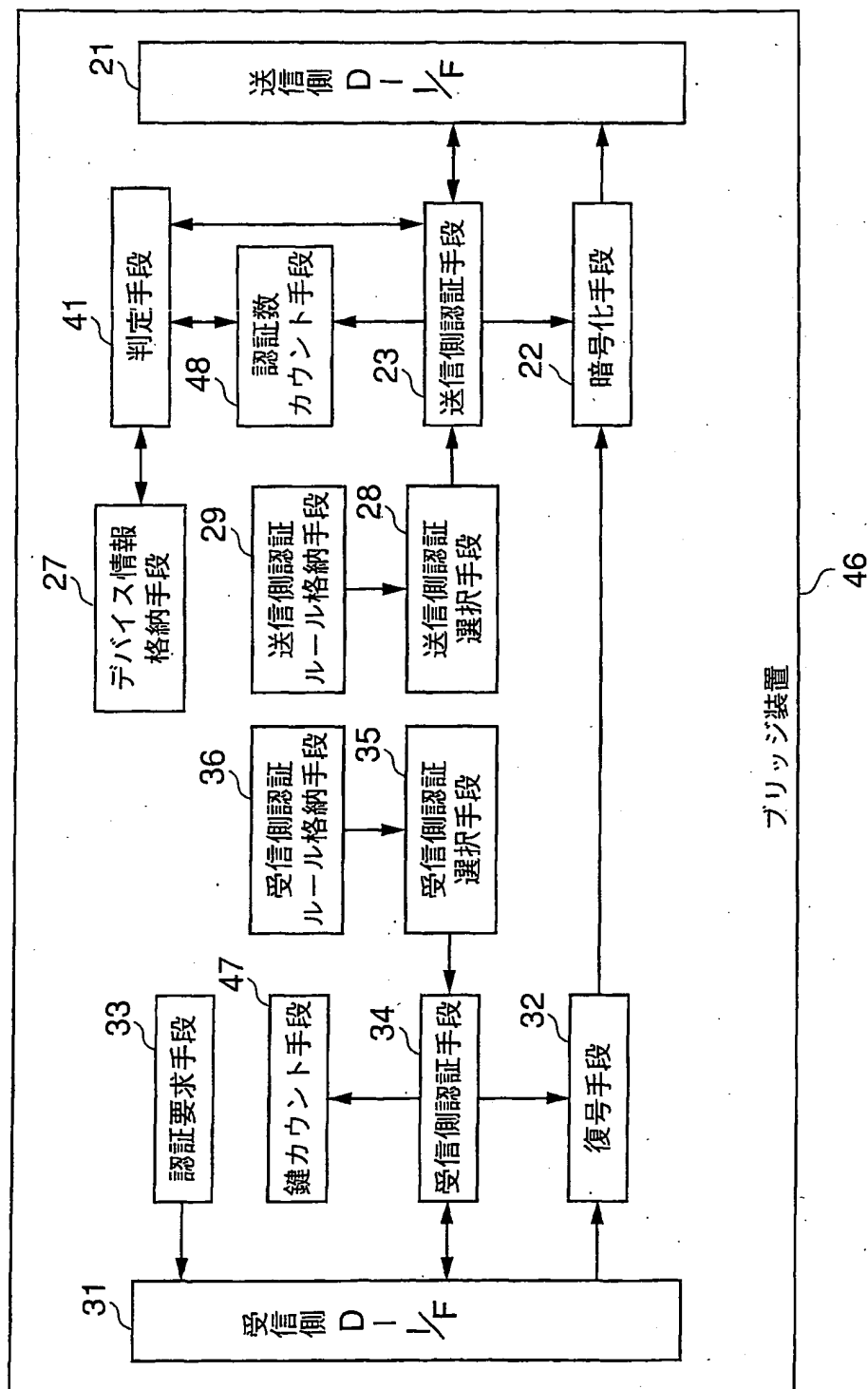
9 / 1 2

第 9 図



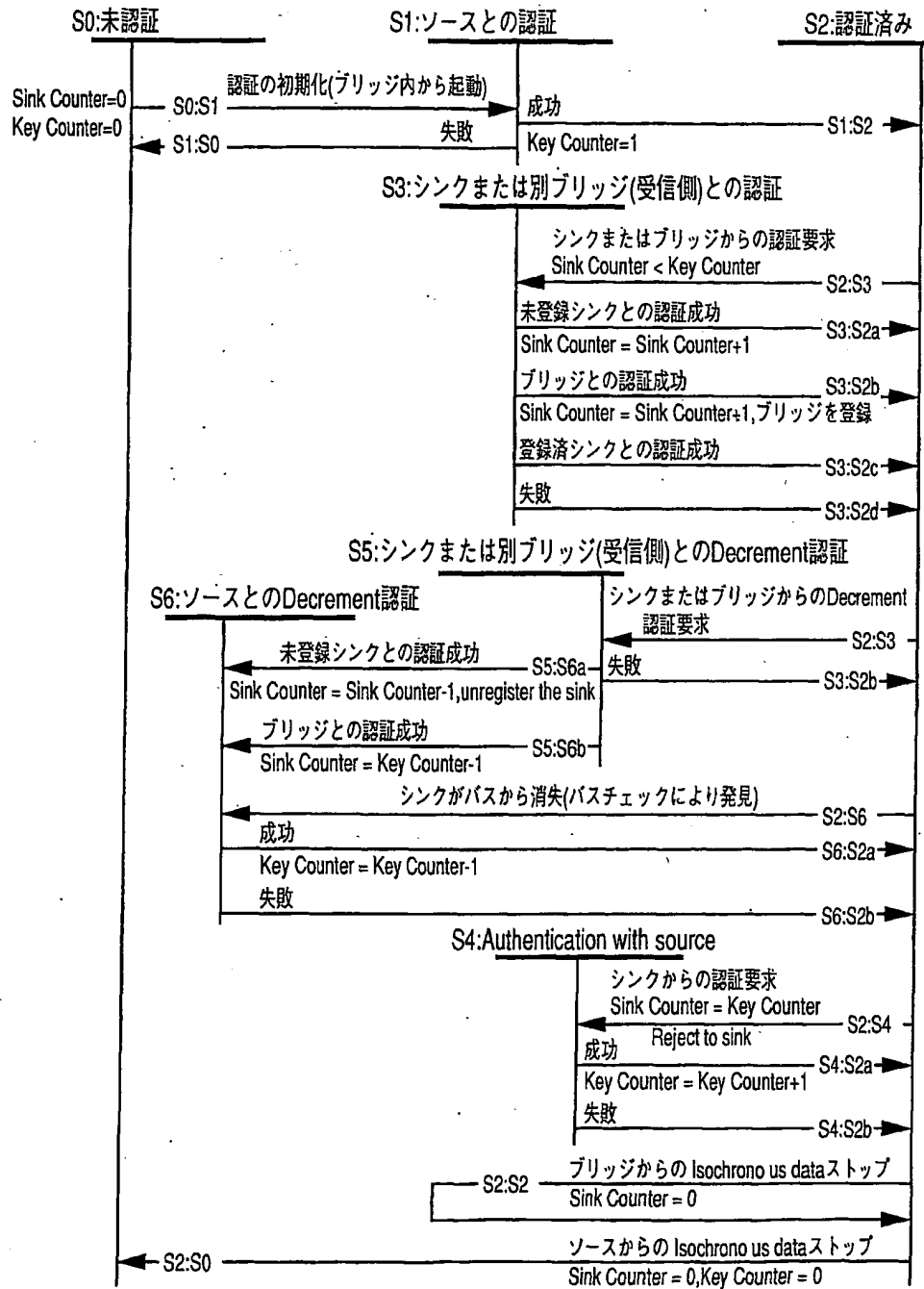
1 0 / 1 2

第 1 0 図



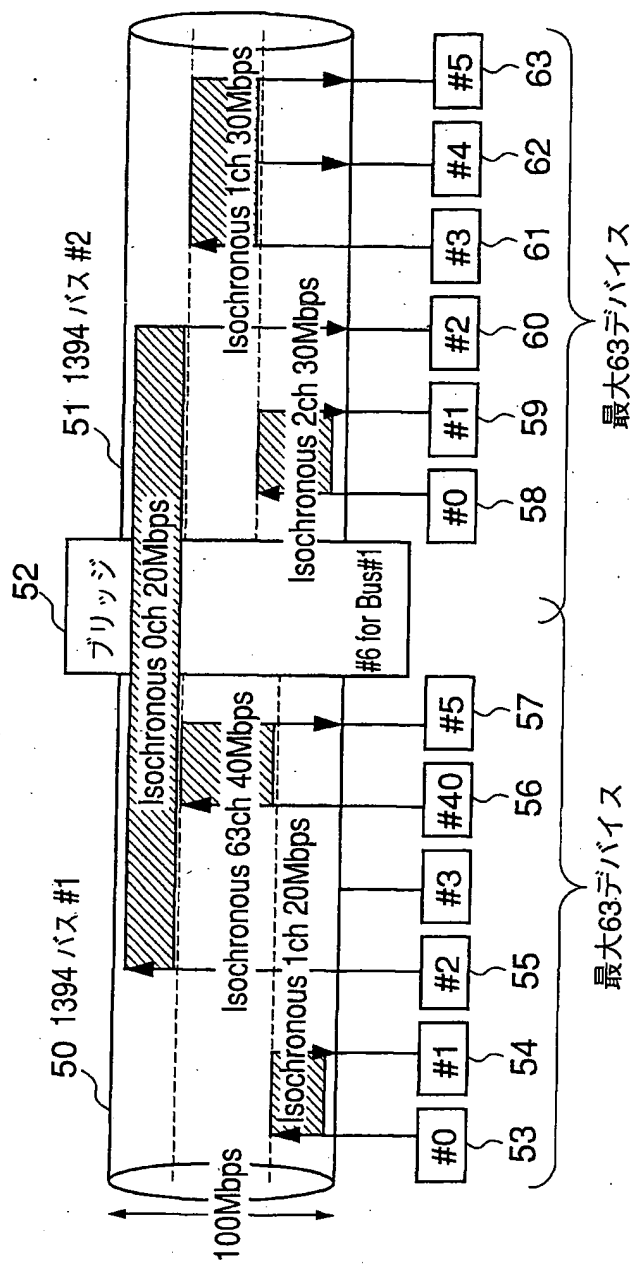
1 1 / 1 2

第 1 1 図



1 2 / 1 2

第 1 2 図



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/08034

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ H04L12/28, G06F13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ H04L12/28, G06F13/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-165376 A (Matsushita Electric Ind. Co., Ltd.), 16 June, 2000 (16.06.00), Figs. 3 to 4, 6 (Family: none)	1-3, 10-12, 15, 16, 18-27, 29, 30, 46, 47, 49-51
A		4-9, 13, 14, 17, 28, 31-45, 48
Y	JP 07-200492 A (CSK Sogo Kenkyusho K.K.), 04 August, 1995 (04.08.95), Fig. 2 (Family: none)	1-3, 10-12, 15, 16, 18-27, 29, 30, 46, 47, 49-51
A		4-9, 13, 14, 17, 28, 31-45, 48

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art


"&" document member of the same patent family

Date of the actual completion of the international search
06 December, 2001 (06.12.01)Date of mailing of the international search report
18 December, 2001 (18.12.01)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int. Cl ⁷ H04L12/28, G06F13/00		
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int. Cl ⁷ H04L12/28, G06F13/00, H04L9/32		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2001年 日本国登録実用新案公報 1994-2001年 日本国実用新案登録公報 1996-2001年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2000-165376 A (松下電器産業株式会社) 16. 6月. 2000 (16. 06. 00) 第3-4図, 第6図 (ファミリーなし)	1-3, 10-12, 15, 16, 18-27, 29, 30, 46, 47, 49-51
A		4-9, 13, 14, 17, 28, 31-45, 48
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に関する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日 06. 12. 01	国際調査報告の発送日 18.12.01	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 中木 努  5X 9299 電話番号 03-3581-1101 内線 3596	

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 07-200492 A (株式会社シーエスケイ) 04. 8月. 1995 (04. 08. 95) 第2図 (ファミリーなし)	1-3, 10-12, 15, 16, 18-27, 29, 30, 46, 47, 49-51
A		4-9, 13, 14, 17, 28, 31-45, 48